

LATHAM & WATKINS

# Outsourcing – Guidance on the Legal and Regulatory Framework

2020

**afme** /  
Finance for Europe

Matheson

BSP



# Contents

---

<b>CONTENTS</b> .....	<b>1</b>
<b>EXECUTIVE SUMMARY</b> .....	<b>3</b>
Scope of this Paper .....	4
<b>KEY THEMES</b> .....	<b>5</b>
Outsourcing Mapping Table .....	6
<b>PART ONE EUROPEAN LEVEL OUTSOURCING GUIDANCE</b> .....	<b>9</b>
EBA Guidelines .....	9
EIOPA guidelines .....	12
<b>PART TWO OTHER EUROPEAN LEVEL CONSIDERATIONS</b> .....	<b>15</b>
Markets in Financial Instruments Directive (2014/65/EU) (“MiFID II”) .....	15
MiFID II Commission Delegated Regulation (EU) 2017/565 .....	16
General Data Protection Regulation (EU) 2016/679.....	19
Directive concerning measures for a high common level of security of network and information systems (EU) 2016/1148.....	21
Capital Requirements Directive (2013/36/EU) (“CRD IV”).....	24
Money Laundering Directive (EU) 2015/849 (“MLD”) .....	25
Benchmarks Regulation (EU) (2016/1011) (“BMR”).....	27
ESMA Guidelines On Certain Aspects Of MIFID Compliance Function Requirements (28 September 2012 (Updated 5 June 2020)) (2012/388) (The “ESMA Guidelines”).....	28
Outsourcing post-brexit: EBA and ECB guidance .....	30
The Revised Payment Services Directive (EU) 2015/2366 .....	32
<b>PART THREE JURISDICTION SPECIFIC GUIDANCE</b> .....	<b>33</b>
France .....	34
Germany .....	39
Ireland .....	46
Italy.....	50
Luxembourg .....	62
Spain.....	66
United Kingdom.....	73
<b>SCHEDULE 1 TEMPLATE OUTSOURCING REGISTER</b> .....	<b>81</b>
<b>SCHEDULE 2 PART A – CHECKLIST FOR CONTRACTUAL REQUIREMENTS UNDER THE EBA GUIDELINES</b> .....	<b>84</b>
<b>SCHEDULE 2 PART B - CHECKLIST FOR CONTRACTUAL REQUIREMENTS UNDER THE CLOUD RECOMMENDATIONS</b> .....	<b>99</b>
<b>SCHEDULE 3 CHECKLIST FOR CONTRACTUAL REQUIREMENTS UNDER THE EIOPA GUIDELINES</b> .....	<b>108</b>
<b>SCHEDULE 4 UK SPECIFIC REGULATION</b> .....	<b>125</b>
<b>SCHEDULE 5 COMPARISON MIFID II DELEGATED REGULATION AND EBA GUIDELINES</b> .....	<b>136</b>
<b>ABOUT THE AUTHORS</b> .....	<b>146</b>
<b>CONTACTS FOR FURTHER ADVICE</b> .....	<b>147</b>

# EXECUTIVE SUMMARY

It is common for firms to outsource certain functions, whether to group entities or to third parties, and firms must comply with a range of regulatory requirements (from different sources) in relation to outsourcing. Compliance and legal teams (both in the first line and the second line) may be responsible for compliance with the regulatory requirements.

With this in mind, members of AFME's Compliance Committee and Compliance Issues working group worked with Latham & Watkins to create this outsourcing reference paper. It consolidates the European legal and regulatory requirements for outsourcing arrangements with group entities and third parties. It also contains information on relevant enforcement decisions. The reference paper is intended to help compliance and legal teams meet their responsibilities in relation to outsourcing arrangements.

The reference paper also considers the relationship between branches and head offices in outsourcing arrangements, and provides information on the requirements and approaches in France, Germany, Ireland, Italy, Luxembourg, Spain and the United Kingdom.

Where appropriate, we may use the paper as a basis for requesting guidance from regulators (EBA, ECB, EU27, UK) in order to support firms' compliance.

Given the regulatory and legislative changes that are expected to occur in relation to firms' outsourcing arrangements, we plan to update this reference paper on an ongoing basis.

*Please note that this Paper is intended for general informational purposes only, and does not provide, and does not constitute, investment, tax, regulatory, business or legal advice to any individual or entity.*

# INTRODUCTION

---

In light of the plethora of legislative change and the increasing regulatory focus on outsourcing in the financial services space, as well as the growing range of sources that need to be taken into account to ensure compliance in this area, this document (the “Paper”) is designed to provide a single reference point for compliance, legal and risk teams within regulated firms of the key legislation, rules, and guidance (including from enforcement cases<sup>1</sup>) that they may wish to consider from an outsourcing perspective. This has become a focus topic in light the growing body of guidance, the need for firms to respond to unforeseen events, increasing reliance on a small range of IT providers (for example, in relation to the cloud), and its interconnectedness to the broader topic of operational resilience.

In particular, it is common for firms to outsource certain functions, whether to group entities or to third parties. The business teams or functions responsible for the outsourcing will be responsible for ensuring compliance with applicable regulatory requirements. There is also a reliance on (i) arrangements set up by group functions, and (ii) other branches within the same legal entity, where there are questions around the extent of application of regulatory requirements, particularly in a Brexit context. The purpose of this Paper is therefore to act as a reference point by drawing together the regulatory requirements and relevant enforcement decisions in relation to outsourcing (and to identify the scope requirements), in order to help risk, business, compliance and legal teams with their role in this respect.

## Scope of this Paper

This Paper is divided into the following three parts:

### **Part One – European Level Outsourcing Guidance**

This part of the Paper provides an overview of the European-wide outsourcing-specific regulatory frameworks laid down by the European Banking Authority (“EBA”) and the European Insurance and Occupational Pensions Authority (“EIOPA”);

### **Part Two – Other European Level Considerations**

This part of the Paper explores, at a high level, the legal and regulatory considerations that should be taken into account (in addition to the specific requirements covered in Part One) when an applicable firm is entering into outsourcing arrangements; and

### **Part Three – Jurisdiction Specific Guidance**

This part of the Paper outlines the jurisdiction-specific considerations required by the financial services regulators in the following countries:

- France;
- Germany;
- Ireland;
- Italy;
- Luxembourg;
- Spain; and
- UK

### **Brexit**

The information contained in this Paper may be subject to change as a result of the ongoing Brexit changes.

---

<sup>1</sup> Please note that certain enforcement cases have been referred to, however, this Paper does not provide an exhaustive list of the enforcement cases relevant to this area.

# KEY THEMES

---

As noted in the introduction above, this Paper covers legislation, rules, guidance, and areas of market or regulatory focus, both at the European-level, and in a number of specific jurisdictions. However, despite the breadth of information in this area, there are a number of over-arching themes which we have identified throughout this Paper, including:

**Increased regulatory focus on outsourcing:** there has been a significant amount of legislative change in relation to outsourcing which has resulted in a commensurate increase in regulatory focus in this area. This is likely to continue, with outsourcing being identified as a key driver of harm in relation to other systemically important areas (such as operational resilience (see below)), and therefore firms should be prepared for on-going regulatory scrutiny in this respect.

**Operational resilience:** Operational resilience is a key focus area for regulators across Europe, at both the national and European level and the COVID-19 crisis has further intensified the regulatory scrutiny and focus in this area. As firms become increasingly dependent on outsourced and third-party service providers and intra-group service providers this has also increased the regulatory focus on outsourcing as a key driver of operational risk. In particular, regulators are concerned to ensure that firms have appropriate arrangements in place to reduce the risk of operational disruption resulting in harm to their clients and/or the wider markets as a result of a failure in relation to their outsourcing arrangements. Accordingly firms should ensure that they consider their outsourcing obligations in this wider context.

**Intra-group and intra-entity arrangements:** We refer to both **intra-group** and **intra-entity** outsourcings throughout this Paper. The term “intra-group” is used to define situations where a firm enters into an outsourcing arrangement with a separate legal entity within the same group (including cross-border outsourcings). This would include a situation where an EEA entity outsources to its UK or third country affiliate. The term “intra-entity” is used to define situations where a firm enters into an outsourcing arrangement within the same legal entity (for example, outsourcing by a UK branch to its EEA head office (which forms part of the same legal entity) or outsourcings between two branches of the same legal entity). In light of Brexit, as well as a general increase in focus on outsourcing by regulators, there is now a significant emphasis on the need for intra-group outsourcing arrangements to meet the same requirements as outsourcings to external third parties (‘third party outsourcings’). Accordingly, firms should not treat intra-group outsourcings as being less risky, or as not being subject to outsourcing requirements, although there will be questions over the real ability to exert influence in practice, reliance and the real ability to move business elsewhere. Firms may however consider the extent to which they influence and control their third-parties, so that risks can be identified and managed effectively. Intra-entity arrangements are generally lower risk than intra-group arrangements, and are not deemed to be outsourcing arrangements for many regulatory requirements, however, firms should still be aware of any regulatory requirements and expectations around such arrangements, particularly in a Brexit context.

**Brexit:** The issue of managing intra-group arrangements has become more prevalent in the Brexit context, in particular where a branch may be subject to different/enhanced outsourcing requirements compared to its head office and where some of the requirements apply intra-entity. This can create issues, in particular where the branch is driving the minimum standards of compliance and where data is required from its head office (or another branch monitored, supervised and documented as an arrangement with the head office) in order to facilitate compliance by the branch (which is a mere beneficiary of a broader arrangement set up by its head office with more limited influence). This issue may also be exacerbated where regulators are seeking to extend the applicable outsourcing requirements in order to ensure that they have adequate oversight/control over the entities that they regulate, resulting in particular in difficulties for firms operating on a cross-border basis.

# Outsourcing Mapping Table

Part One – European Level Outsourcing Guidance					
EBA Guidelines					
Applies to outsourcing to third-parties	✓	Applies to intra-group outsourcings	✓	Applies to intra-entity outsourcings	✗
Brexit Implications		EU Level 3 materials will not be onshored, and, accordingly, the EBA Guidelines will not form part of UK retained law. The UK regulators have made clear, however, that their supervisory expectations in respect of Guidelines issued by the European Supervisory Authorities will remain the same. Accordingly, they will expect firms (including UK branches of EEA firms), financial institutions and other market participants operating, or intending to operate, in the United Kingdom to continue to apply the EBA Guidelines, to the extent that they remain relevant, as they did before exit subject to the need to interpret these considering Brexit and the associated legislative changes that are being made to ensure the UK regulatory framework operates appropriately after the end of the transition period.			
EIOPA Guidelines					
Applies to outsourcing to third-parties	✓	Applies to intra-group outsourcings	✓	Applies to intra-entity outsourcings	✗
Brexit Implications		The FCA has notified EIOPA that the EIOPA Guidelines are not applicable to regulated activities within the UK's jurisdiction, as they will enter into force on 1 January 2021, after the EU withdrawal transition period ends. The FCA will continue to apply the FCA FG16/5 Guidance for firms outsourcing to the cloud and other third-party IT services in the UK. The FCA has stated that they will keep this guidance under review and, where appropriate, consult to update this to ensure it remains consistent with relevant international standards.			
Part Two – Other European Level Considerations					
MiFID II					
Applies to outsourcing to third-parties	✓	Applies to intra-group outsourcings	✓	Applies to intra-entity outsourcings	✗
Brexit Implications		SYSC 8.1.11 will be amended as part of the onshoring exercise such that the FCA will be the sole competent authority to supervise the compliance of the performance of the relevant outsourced activities. This will take effect when the transition period ends and will also apply to firms (including UK branches of EEA firms) with temporary permission. Aside from supervision matters and the provision of information to the FCA, firms with temporary permission will be able to rely on 'substituted compliance' until they exit the temporary permission regime.			
MiFID II Delegated Regulation					
Applies to outsourcing to third-parties	✓	Applies to intra-group outsourcings	✓	Applies to intra-entity outsourcings	✗
Brexit Implications		The MiFID II Delegated Regulation will be onshored with a UK scope. Firms with temporary permission (including UK branches of EEA firms) will need to comply with the UK specific requirements but can rely on 'substituted compliance' until they exit the temporary permission regime.			

GDPR					
Applies to outsourcing to third-parties	✓	Applies to intra-group outsourcings	✓	Applies to intra-entity outsourcings	✓
Brexit Implications		The GDPR, which is currently supplemented and tailored by the Data Protection Act 2018 in the UK, will be onshored into UK law as the 'UK GDPR' at the end of the transition period. Whilst initially the core data protection principles, obligations and rights will remain the same under UK GDPR, it is important to note that there will be two distinct regimes (i.e., EU GDPR and UK GDPR) that could diverge over time. In the absence of a decision from the European Commission that UK law provides an adequate level of data protection, from the end of the transition period, EU GDPR transfer rules will apply to any data coming from the EEA into the UK (including via branches). It is currently expected that transfers of data from the UK to the EU will, at least initially, be able to continue on the basis of the UK recognising the EU GDPR as providing an adequate level of data protection.			
NIS Directive					
Applies to outsourcing to third-parties	✓	Applies to intra-group outsourcings	✓	Applies to intra-entity outsourcings	✓
Brexit Implications		The Network and Information Systems Regulations 2018 (SI 2018/506) will continue to apply in the UK after the end of the transition period.			
CRD IV					
Applies to outsourcing to third-parties	✓	Applies to intra-group outsourcings	✓	Applies to intra-entity outsourcings	✓
Brexit Implications		Any intra-group or intra-entity outsourcings that impact any of the requirements under CRD IV should be taken into account in the same way as for third-party outsourcings and this will continue to be the case after the transition period ends.			
MLD					
Applies to outsourcing to third-parties	✓	Applies to intra-group outsourcings	✓	Applies to intra-entity outsourcings	✗
Brexit Implications		UK firms will no longer be able to rely automatically on customer due diligence carried out by a person carrying on business in the EEA who is subject to national legislation implementing the MLD. However, the provision allowing reliance on a person carrying on business in a third country who is subject to requirements that are equivalent to the customer due diligence requirements of the MLD will be maintained, so presumably UK firms will continue to be able to rely on customer due diligence carried out by EEA businesses under this provision (subject to any relevant considerations applicable to particular countries).			
BMR					
Applies to outsourcing to third-parties	✓	Applies to intra-group outsourcings	✓	Applies to intra-entity outsourcings	✗
Brexit Implications		BMR will be onshored with a UK-only scope. From the end of the transition period, the FCA will be the sole competent authority in relation to the Article 10 requirements applicable to outsourcings by a benchmark administrator.			



ESMA Guidelines (including cloud proposals)					
Applies to outsourcing to third-parties	✓	Applies to intra-group outsourcings	✓	Applies to intra-entity outsourcings	✗
Brexit Implications		EU Level 3 materials will not be onshored, and, accordingly, the ESMA Guidelines will not form part of UK retained law. Firms operating, or intending to operate, in the United Kingdom should however continue to apply ESMA Guidelines, to the extent that they remain relevant, as they did before exit. The ESMA Guidelines will need to be interpreted in light of the Brexit changes that are being made in the UK to ensure that the regulatory framework operates appropriately.			
EBA & ECB Brexit guidance					
Applies to outsourcing to third-parties	✓	Applies to intra-group outsourcings	✓	Applies to intra-entity outsourcings	✗
Brexit Implications		The EBA and ECB Brexit guidance will continue to be relevant to EU27 firms and their branches after the end of the transition period.			
PSD2					
Applies to outsourcing to third-parties	✓	Applies to intra-group outsourcings	✓	Applies to intra-entity outsourcings	✓
Brexit Implications		<p>PSD2 is incorporated into UK law through the Payment Services Regulations 2017 (PSRs) and will therefore continue to apply in the UK from the end of the transition period. Certain onshoring changes will be made to the PSRs in order to ensure that they function appropriately after the end of the transition period, including shifting responsibility for all binding technical standards from the European Supervisor Authorities to the UK regulators. Firms will continue to be supervised by the FCA under the PSRs and matters relating to passporting rights, including home state notifications, will be deleted.</p> <p>The PSRs are subject to a temporary permission regime. The FCA will become the sole competent authority for any UK business of an EEA firm operating under the temporary permissions regime.</p>			
PRA Proposals (CP 30/19)					
Applies to outsourcing to third-parties	✓	Applies to intra-group outsourcings	✓	Applies to intra-entity outsourcings	✓
Brexit Implications		The final policy on the proposals in CP 30/19 is expected in Q1 2021. The current proposals purport to apply to UK branches of EEA firms and, accordingly, clarification is required for firms with temporary permission that the requirements will apply upon exiting the temporary permissions regime as there are some differences compared to the EBA Guidelines which may require further action by firms to implement.			



# PART ONE

## EUROPEAN LEVEL OUTSOURCING GUIDANCE

---

### EBA Guidelines

The EBA published a final report on its draft guidelines on outsourcing arrangements on 25 February 2019 (the “**EBA Guidelines**”), which create new obligations for financial, payment, and electronic money institutions. The EBA Guidelines also replace and incorporate the EBA’s final recommendations on outsourcing to cloud service providers (the “**Cloud Recommendations**”).

### Who does it apply to?

The EBA Guidelines apply to all financial institutions that are:

- Within the scope of the EBA’s mandate, including credit institutions;
- Investment firms subject to Directive (EU) 2013/36 IV (CRD IV);
- Payment institutions; and
- Electronic money institutions.

### Timing

- The EBA Guidelines came into force on 30 September 2019.

### Scope

Any outsourcing arrangements entered into, reviewed, or amended by an institution subject to the EBA Guidelines after 30 September 2019 must comply with the EBA Guidelines. Institutions must also update all existing outsourcing arrangements in line with the EBA Guidelines by 31 December 2021. The EBA Guidelines distinguish between those arrangements involving functions they consider “critical or important” (defined below), and all others. Both types are subject to the EBA Guidelines but with different degrees of scrutiny.

While the EBA Guidelines’ internal governance requirements apply across all outsourcing arrangements, specific considerations are applicable where the outsourcing is to the cloud. Please see Schedule 2 Part B for cloud - specific considerations.

### Key definitions

- “**critical or important function**” means any function that is considered critical or important as set out in Section 4 of the EBA Guidelines:

Institutions and payment institutions should always consider a function as critical or important in the following situations:

- where a defect or failure in its performance would materially impair:
  - their continuing compliance with the conditions of their authorisation or its other obligations under Directive 2013/36/EU (“**CRD IV**”), Regulation (EU) No 575/2013 (the “**Capital Requirements Regulation**”), Directive 2014/65/EU (MiFID II), Directive (EU) 2015/2366 (the “**Payment Services Directive**”) and Directive 2009/110/EC (the “**E-Money Directive**”) and their regulatory obligations;
- their financial performance; or
- the soundness or continuity of their banking and payment services and activities;
  - when operational tasks of internal control functions are outsourced, unless the assessment establishes that a failure to provide the outsourced function or the inappropriate provision of the outsourced function would not have an adverse impact on the effectiveness of the internal control function; or
  - when they intend to outsource functions of banking activities or payment services to an extent that would require authorisation by a competent authority, as referred to in Section 12.1 (of the EBA Guidelines);
- “**function**” means any processes, services or activities; and
- “**outsourcing**” means an arrangement of any form between an institution, a payment institution or an electronic money institution and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the institution, the payment institution or the electronic money institution itself.

## Internal Governance/Overarching Requirements

Institutions must adopt a high-level risk management framework based on the EBA Guidelines. In particular, institutions must:

- Ensure that accountability and oversight remains with the institution's management;
- Maintain an outsourcing policy (the "**Policy**", as further described below) that complies with the EBA Guidelines;
- Manage conflicts of interest in a systematic and regular manner;
- Maintain a business continuity plan that complies with the EBA Guidelines;
- Conduct regular internal audits; and
- Create and maintain a register of all outsourcing arrangements, listing the categories of information required by the EBA Guidelines (the "**Register**", as further described below).

### Institutions are expected to:

- Conduct pre-outsourcing analysis before entering into any new outsourcing arrangements (e.g., identify risks) and consider any notification requirements (please see 'notification requirements' below for further details);
- Undertake due diligence (e.g., ascertain the service provider's expertise, capacity, business reputation, and security of systems);
- Ensure that the contract for any new outsourcing arrangement, especially of critical or important functions, contains the features prescribed by the EBA Guidelines (e.g., full audit rights, specific termination rights). Please see 'contractual requirements' below for further details; and
- Plan an exit strategy in relation to each outsourcing arrangement.

## Outsourcing Policy

The EBA Guidelines further set out requirements that institutions should follow in respect of the Policy, in particular institutions should:

- Include the main phases of outsourcing arrangements and define the principles, responsibilities, and processes;
- Ensure that the Policy meets the requirements in Section 9 of the EBA Guidelines in relation to business continuity planning;
- Cover the responsibilities of their organisation's management and involvement of business lines, internal control functions, and other key roles in respect of outsourcing;
- Describe the planning of outsourcing arrangements, including as a minimum:
  - Any business requirements;
  - The criteria for critical or important functions;
  - Risk and potential conflicts of interest;
  - Business continuity plans; and
  - The approval process of new outsourcing arrangements;
- Detail in the Policy how outsourcing arrangements will be implemented, monitored and managed (e.g., on-going review of service provider's performance, procedures for notification of changes, independent audit, and renewal processes);
- Set out documentation and record-keeping requirements, which must be in line with the EBA Guidelines;
- Differentiate between:
  - Outsourcing of critical or important functions and all others;
  - Outsourcing to service providers that are authorised by a competent authority and those that are not;
  - Outsourcing within the same group or institutional protection scheme and to third parties; and
  - Outsourcing to service providers in an EU member state and those in third countries;
- Account for the institution's risk profile, ability to oversee the service provider, business continuity measures and performance of business activities.

## Outsourcing register

The EBA Guidelines prescribe that all institutions subject to the EBA Guidelines must maintain the Register for all their outsourcing arrangements. This is a new requirement that was not included in the EBA Guidelines' predecessor.

For assistance with preparing the Register, please see the template set out at Schedule 1.

## Contractual requirements

The EBA Guidelines contain a number of contractual requirements that should be considered when negotiating outsourcing agreements. A contractual requirements checklist is set out in Schedule 2, Part A of this Paper. In the case of cloud outsourcing, the requirements in Schedule 2 Part B should also be considered. Paragraph 1 of the EBA Guidelines states that “competent authorities must make every effort to comply with the guidelines” (i.e., it is not expressed as an absolute obligation to comply in full). Due to the relatively recent introduction of the EBA Guidelines, we have yet to see how the regulators will interpret this and whether they will expect to see strict compliance with each of the contractual requirements or whether they will accept negotiated positions.

## Application to intra-group/intra-entity arrangements

### Intra-group arrangements

The EBA Guidelines also apply to intra-group outsourcing arrangements. Intra-group outsourcing was considered during the public consultation for the EBA Guidelines, which focused particularly on the concern that, due to the granularity of the requirements set forth within the EBA Guidelines, intra-group outsourcing would be hindered. The EBA responded, noting that “institutions and members of the management body are responsible for ensuring robust governance arrangements and managing all risks...[t]he responsibility cannot be delegated”. Each individual institution therefore must be cognisant of its own responsibilities, notwithstanding a centralised, consolidated group arrangement or policy. For institutions subject to the EBA Guidelines that have historically placed reliance on a centralised procurement function or service entity, this responsibility may require internal review.

Institutions that outsource important or critical functions intra-group must be able to demonstrate to regulators that:

- The group entity is selected based on objective reasons;
- The conditions of the outsourcing arrangement are set at arm’s length; and
- The conditions deal explicitly with any conflicts of interest the outsourcing arrangement may pose.

Institutions must also be cognisant of the fact that outsourcing must not lead to a situation in which a financial institution becomes an empty shell that lacks the substance to remain authorised. To counter this outcome, outsourcing entities must retain sufficient resources and a robust operational and governance framework to carry out effectively their own management and oversight responsibilities. Increased costs of such compliance will need to be factored into business cases when considering the merits of an outsourcing arrangement.

### Intra-entity arrangements

Services provided by “non-independent parts of an institution”, such as branches are not an “outsourcing” (as defined in the key definitions above) and therefore fall outside the scope of the EBA Guidelines.

## European level supervision

Whilst the EBA Guidelines will be supervised and enforced at national level, banks or banking groups that fulfil certain significance criteria (significant institutions) are also subject to direct supervision by the European Central Bank (“**ECB**”). ECB banking supervision aims to ensure that banks take full advantage of innovative advancements while maintaining a secure environment, with risks duly monitored and mitigated. To this end, it has embedded the revised EBA framework in its supervisory standards, taking this into account in the context of its ongoing supervision. The ECB is also committed, as part of its banking supervision, to implement the EBA Guidelines and will monitor the actions taken by banks to adapt their outsourcing arrangements accordingly.

## Notification requirements

There are several notification requirements contained within the EBA Guidelines which should be noted:

- institutions must adequately and timely inform the competent authorities about planned outsourcings of critical or important functions, including where an outsourced function becomes critical or important;
- if the location where the critical or important function is provided changes, there is a requirement for the service provider to notify the institution;
- there is a communication requirement by the service provider of any development that might have a material impact on the service provider’s ability to effectively carry out the critical or important function;
- there is an obligation on the service provider to inform of any planned sub-outsourcing; and
- before a planned on-site visit, competent authorities should provide reasonable notice to the service provider.

## EIOPA guidelines

On 31 January 2020, EIOPA published a final report setting out its guidelines on outsourcing to cloud service providers (the “**EIOPA Guidelines**”).

EIOPA has considered the EBA Guidelines and Cloud Recommendations in preparation of the EIOPA Guidelines which means that there is a certain degree of similarity in these requirements.

Note that the EIOPA Guidelines will not be applicable to regulated activities within the UK’s jurisdiction, as they will enter into force on 1 January 2021, after the end of the transition period. UK branches of EEA firms will need to consider whether there is any impact on their activities as a result of the obligations applicable to their Head Office, however, as noted below, intra-entity outsourcing does not fall within the scope of the EIOPA Guidelines.

### Who does it apply to?

The EIOPA Guidelines apply to insurance and reinsurance undertakings. Parts of the EIOPA Guidelines are also addressed to competent authorities.

### Timing

The EIOPA Guidelines are set to come into force on 1 January 2021. All cloud outsourcing arrangements entered into or amended by undertakings on or after this date must comply with the EIOPA Guidelines. Undertakings must also review and amend all existing cloud outsourcing arrangements in accordance with the EIOPA Guidelines by 31 December 2022.

### Scope

The EIOPA Guidelines are intended to provide guidance to insurance and reinsurance undertakings on how the outsourcing provisions in the Solvency II Directive and the Solvency II Delegated Regulation (both as defined below) need to be applied in the case of outsourcing to cloud service providers.

### Key definitions

“**cloud services**” means 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 cloud service provider interaction;

- “**community cloud**” means cloud infrastructure available for the exclusive use by a specific community of undertakings, e.g., several undertakings of a single group;
- “**hybrid cloud**” means cloud infrastructure that is composed of two or more distinct cloud infrastructures;
- “**private cloud**” means cloud infrastructure available for the exclusive use by a single undertaking;
- “**public cloud**” means cloud infrastructure available for open use by the general public;
- “**Solvency II Delegated Regulation**” means Commission Delegated Regulation (EU) No 2015/35; and
- “**Solvency II Directive**” means Directive 2009/138/EC – Insurance and Reinsurance Directive (recast) (Solvency II).

### Internal governance/overarching requirements

The EIOPA Guidelines set out a number of rules that undertakings must consider as part of their internal governance before engaging in cloud outsourcings that are subject to the EIOPA Guidelines. To meet these rules, undertakings are expected to:

- Ensure that any decision to outsource critical or important operational functions or activities to cloud service providers is made by the undertaking’s administrative, management or supervisory body (“**AMSB**”), and considering the following risks by way of a thorough assessment:
  - Information and communication technology;
  - Business continuity;
  - Legal and compliance;
  - Concentration; and
  - If applicable, data migration;
- Update the undertaking’s written outsourcing policy for cloud computing specificities, at least in respect of:
  - The roles and responsibilities of each function (in particular **AMSB**, IT function, information security, compliance function, risk management function and internal audit);
  - Reporting procedures and processes for the implementation, monitoring and management of the outsourcing arrangement;
  - Oversight of the cloud services, such as risk assessments and due diligence, monitoring and service controls, and security standards;



- Contractual requirements;
- Documentation requirements and notification to the supervisory authority; and
- Documented exit strategies;
- Assess and determine whether the outsourcing is considered an outsourcing of critical or important operational functions (with the same meaning as under the Solvency II Directive), and whether it affects the undertaking's risk profile. The assessment should consider a variety of factors, including the impact of any material disruptions, the undertaking's ability to manage risks, comply with regulatory requirements and conduct audits, and the size and complexity;
- Conduct regular audits in line with Section 8 of EIOPA's Guidelines on Systems of Governance, and setting up monitoring and oversight mechanisms to monitor the cloud service provider's performance, security measures and adherence to the outsourcing contract on an on-going basis; and
- Develop exit strategies and ensure that these are aligned with the termination and exit provisions of the outsourcing agreement.

Before entering an outsourcing arrangement, undertakings should be in accordance with the EIOPA Guidelines:

- Carry out a pre-outsourcing analysis:
  - Assessing if the outsourcing concerns a critical or important function;
  - Identifying and assessing all relevant risks and potential conflicts of interest; and
  - Undertaking due diligence on the cloud service provider;
- For any cloud outsourcing, assess the operational and reputational risks and, for any outsourcing of critical or important operational functions, conduct a risk assessment (which must be repeated in certain circumstances, e.g., any significant changes or significant deficiencies), which at a minimum considers risks arising from:
  - The type of cloud service and deployment model;
  - Migration and implementation;
  - The sensitivity of the systems and data, and any required security measures;
  - The cloud service provider's location, with respect to data processing and storing;
  - Political stability and security situation in the relevant jurisdictions, within or outside the EU, where the data will likely be stored (including the laws on data protection, law enforcement and insolvency law provisions);
  - Sub-outsourcing by the cloud service provider; and
  - Concentration risk from outsourcing to a dominant, or several connected, cloud service providers;
- Ensure that the contract for any new outsourcing arrangement, especially outsourcing arrangements for critical or important functions, contains the features prescribed by the EIOPA Guidelines. Please see 'contractual requirements' below for further details.

Undertakings are also expected to provide written notification to the supervisory authority prior to the outsourcing of critical or important functions or activities, as well as notification of any subsequent material developments with respect to those functions or activities (as per Article 49(3) of the Solvency II Directive). The written notification should include at least the following information:

- A brief description of the function or activity being outsourced, and the reasons why it is considered critical or important;
- The agreement's relevant dates; as applicable, the start date, renewal date, end date and notice periods;
- The governing law of the agreement;
- Details about the cloud service provider (e.g., name, corporate registration number, and whether it has a parent company or group);
- Details about the services, deployment models, nature of data and its storage locations; and
- The date of the most recent assessment of the criticality or importance of the function or activity.

The EIOPA Guidelines also prescribe that undertakings should keep records of information on all of its outsourcing arrangements with cloud service providers. The records should include terminated cloud outsourcing arrangements subject to appropriate retention periods and institutions must be prepared to make the records available to its competent authority upon its request, along with a copy of the outsourcing agreement. For outsourcings of non-critical or important functions, undertakings should define the information to be recorded based on the nature, scale and complexity of the risks inherent in the services; for outsourcings of critical or important functions, undertakings should record the information based on the prescribed list. For assistance with record-keeping for outsourcings of critical or important functions, please see rows 1 and 2 of Schedule 3 for the full list of required information.

## Contractual requirements

The EIOPA Guidelines distinguish between those arrangements they consider "outsourcing of critical or important functions", and all others. Both types are subject to the EIOPA Guidelines but non-critical or important arrangements do not face the same level of scrutiny. The EIOPA Guidelines contain a number of contractual requirements that undertakings should consider when preparing cloud outsourcing agreements. Latham & Watkins have prepared a contractual requirements checklist which is set out in full in Schedule 3 and seeks to provide a reference to the key contractual requirements for negotiating and drafting purposes.



## Application to intra-group/intra-entity arrangements?

### Intra-group arrangements

The EIOPA Guidelines apply to intra-group arrangements

In the group context, the EIOPA Guidelines, in particular, envisage that several undertakings that are part of the same group may use the same cloud outsourcing arrangement (as recipients of the cloud services). For example, as part of their documentation requirements under Guideline 5 of the EIOPA Guidelines, undertakings must keep a record of any insurance or reinsurance undertakings and other undertakings that are within the scope of the prudential consolidation and that make use of the cloud services. The impact assessment that is annexed to the EIOPA Guidelines further considers that group undertakings may wish to fulfil certain requirements as a group rather than separate undertakings. Under Guideline 4 of the EIOPA Guidelines, an undertaking must declare whether the service is being provided intra-group through a group service provider.

The EIOPA Guidelines also state that in case of intra-group outsourcing and sub-outsourcing to cloud service providers, the applicable guidelines should be applied in conjunction with the provisions of EIOPA Guidelines on System of Governance on intra-group outsourcing.

### Intra-entity arrangements

The EIOPA Guidelines define a service provider to an outsourcing as a “third party entity”. Consequently, intra - entity outsourcing does not fall within scope of the EIOPA Guidelines.

## Notification Requirements

There are several notification requirements contained within the EIOPA Guidelines, which should be noted:

- if the location where relevant data will be stored and processed is to change, there is a requirement to notify the undertaking (para 37(f));
- the cloud service provider must provide reports that are relevant for the undertaking’s internal audit function (para 37(j));
- before a planned on-site visit, the party exercising its right of access should provide prior notice to the relevant business premise (para 45); and
- the cloud service provider must inform the undertaking of any planned significant changes to the sub - contractors or the sub-outsourced services that might affect the ability of the service provider to meet its obligations under the cloud outsourcing agreement (para 50(d)).

# PART TWO

## OTHER EUROPEAN LEVEL CONSIDERATIONS

---

### Markets in Financial Instruments Directive (2014/65/EU) (“MiFID II”)

MiFID II sets out a broad framework in relation to outsourcing and is supplemented by the MiFID II Commission Delegated Regulation (EU) 2017/565 (the “**MiFID II Delegated Regulation**”), which contains directly applicable outsourcing requirements (we have covered the MiFID II Delegated Regulation separately below).

#### Who does it apply to?

The relevant provisions apply to investment firms, as defined under MiFID II. Under MiFID II, an “**investment firm**” is any legal person whose regular occupation or business is the provision of one or more investment services to third parties and/or the performance of one or more investment activities on a professional basis.

#### Timing

MiFID II has been in force since 3 January 2018.

#### Internal governance/overarching requirements

The requirements under MiFID II (Article 16(5)), include:

- When outsourcing the performance of operational functions that are critical for the provision of continuous and satisfactory service to clients and the performance of investment activities on a continuous and satisfactory basis, an investment firm must take reasonable steps in order to avoid undue operational risk;
- An investment firm may not outsource important operational functions so as to impair the quality of its internal controls and its regulator’s ability to monitor the firm’s compliance; and
- An investment firm must also have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective “control and safeguard” arrangements for information processing systems.

#### Application to intra-group/intra-entity arrangements

These requirements apply to intra-group/intra-entity arrangements, however, to the extent that the firm and the service provider are members of the same group, the firm may take into account the extent to which it controls the service provider or has the ability to influence its actions.

##### Intra-group arrangements

These requirements apply to intra-group arrangements, however, to the extent that the firm and the service provider are members of the same group, the firm may take into account the extent to which it controls the service provider or has the ability to influence its actions.

##### Intra-entity arrangements

Outsourcing is defined in the MiFID II Delegated Regulation as “an arrangement of any form between an investment firm and a service provider by which that service provider performs a process, a service or an activity *which would otherwise be undertaken by the investment firm itself*” (emphasis added). Under an intra-entity arrangement an investment firm continues to undertake the service itself and therefore falls outside the scope of these rules.

# MiFID II Commission Delegated Regulation (EU) 2017/565

The MiFID II Delegated Regulation supplements MiFID II in relation to, amongst other things, organisational requirements and operating conditions for investment firms. This includes certain provisions relating to outsourcing.

## Who does it apply to?

The relevant provisions apply to investment firms, as defined in relation to MiFID II (above).

## Timing

Implemented on 25 April 2016, in force with MiFID II from 3 January 2018.

## Key definitions

“**critical or important functions**” means an operational function where a defect or failure in its performance would materially impair the continuing compliance of an investment firm with the conditions and obligations of its authorisation or its other obligations under MiFID II, or its financial performance, or the soundness or the continuity of its investment services and activities.

## Internal governance/overarching requirements

The MiFID II Delegated Regulation requirements, include:

- Under Article 30(1) of the MiFID II Delegated Regulation, investment firms must determine whether an operational function is critical or important by assessing whether a defect or failure in the performance of the outsourced service would materially impair its:
  - Compliance with the conditions and obligations of its authorisation or its other obligations under MiFID II;
  - Its financial performance or soundness; or
  - The continuity of its investment services and activities.
- Under Article 31(1) of the MiFID II Delegated Regulation, when outsourcing critical or important operational functions, an investment firm remains fully responsible for discharging all its obligations under MiFID II. Therefore, the firm must ensure it has full oversight of such outsourced services.
- Under Article 31(1)(a) of the MiFID II Delegated Regulation, investment firms that are outsourcing critical or important operational functions should ensure:
  - The outsourcing does not result in the delegation by senior management of its responsibility;
  - The relationship (and accompanying obligations) of the investment firm towards its clients under MiFID II is not altered;
  - The conditions with which the investment firm must comply in order to be authorised in accordance with Article 5 of MiFID II, and to remain compliant, are not undermined; and
  - None of the other conditions subject to which the firm’s authorisation was granted are removed or modified.
- Under Article 31(2) of the MiFID II Delegated Regulation, investment firms should exercise due skill, care, and diligence when entering into, managing, or terminating any outsourcing arrangement for a critical or important operational function.
- Under Article 31(2) of the MiFID II Delegated Regulation, investment firms should take necessary steps to ensure that the following conditions are satisfied:
  - The service provider has the ability, capacity, sufficient resources, appropriate organisational structure supporting the performance of the outsourced functions, and any authorisation required by law to perform the outsourced functions reliably and professionally;
  - The service provider carries out the outsourced services effectively and in compliance with applicable law and regulatory requirements, and to this end the firm has established methods and procedures for assessing the standard of performance of the service provider and for reviewing on an ongoing basis the services provided by the service provider;
  - The service provider properly supervises the carrying out of the outsourced functions, and adequately manages the risks associated with the outsourcing;
  - Appropriate action is taken where it appears that the service provider may not be carrying out the functions effectively or in compliance with applicable laws and regulatory requirements;
  - The investment firm effectively supervises the outsourced functions or services and manages the risks associated with the outsourcing and to this end the firm retains the necessary expertise and resources to supervise the outsourced functions effectively and to manage those risks;
  - The service provider has disclosed to the investment firm any development that may have a material impact on its ability to carry out the outsourced functions effectively and in compliance with applicable laws and regulatory requirements;



- The investment firm is able to terminate the arrangement for outsourcing where necessary, with immediate effect when this is in the interests of its clients, without detriment to the continuity and quality of its provision of services to clients;
  - The service provider cooperates with the competent authorities of the investment firm in connection with the outsourced functions;
  - The investment firm, its auditors, and the relevant competent authorities have effective access to data related to the outsourced functions, as well as to the relevant business premises of the service provider, where necessary for the purpose of effective oversight in accordance with this article, and the competent authorities are able to exercise those rights of access;
  - The service provider protects any confidential information relating to the investment firm and its clients;
  - The investment firm and the service provider have established, implemented and maintained a contingency plan for disaster recovery and periodic testing of backup facilities, where that is necessary having regard to the function, service or activity that has been outsourced; and
  - The investment firm has ensured that the continuity and quality of the outsourced functions or services are maintained in the event of termination of the outsourcing either by transferring the outsourced functions or services to another third party, or by performing them itself.
- Under Article 31(3) of the MiFID II Delegated Regulation:
    - The respective rights and obligations of the investment firm and of the service provider should be clearly allocated and set out in a written agreement;
    - The investment firm should ensure that the written agreement retains the firm's instruction and termination rights, its rights of information, and its right to inspect and access books and premises; and
    - The written agreement should ensure that the outsourcing by the service provider only takes place with the consent, in writing, of the investment firm.
  - Under Article 31(4)&(5) of the MiFID II Delegated Regulation, where an investment firm outsources to a service provider in a third country functions related to the investment service of portfolio management provided to clients, the firm should ensure that:
    - The service provider is authorised or registered in its home country to provide that service and is effectively supervised by a competent authority in that third country; and
    - There is an appropriate cooperation agreement between the competent authority of the investment firm and the supervisory authority of the service provider.
    - The cooperation agreement must ensure that competent authorities of the investment firm are, at least, able to:
      - Obtain on request the information necessary to carry out their supervisory tasks pursuant to MiFID II and Regulation (EU) No 600/2014 ("MiFIR");
      - Obtain access to the documents relevant for the performance of their supervisory duties maintained in the third country;
      - Receive information from the supervisory authority in the third country as soon as possible, for the purpose of investigating apparent breaches of the requirements of MiFID II and its implementing measures and MiFIR; and
      - Cooperate with regard to enforcement, in accordance with the national and international law applicable to the supervisory authority of the third country and the competent authorities in the European Union, in cases of breach of the requirements of MiFID II and its implementing measures and relevant national law.
  - Recital 44 of the MiFID II Delegated Regulation clarifies that the outsourcing of investment services or activities or critical and important functions is capable of constituting a material change of the conditions for the authorisation of the investment firm, as referred to in Article 21(2) of MiFID II. If such outsourcing arrangements are to be put in place after the investment firm has obtained an authorisation, those arrangements should be notified to the competent authority where required.

## Application to intra-group/intra-entity arrangements

### Intra-group arrangements

These requirements apply to intra-group arrangements, however, to the extent that the firm and the service provider are members of the same group, the firm may take into account the extent to which the firm controls the service provider or has the ability to influence its actions.

### Intra-entity arrangements

Outsourcing is defined in the MiFID II Delegated Regulation as "an arrangement of any form between an investment firm and a service provider by which that service provider performs a process, a service or an activity *which would otherwise be undertaken by the investment firm itself*" (emphasis added). Under an intra-entity arrangement an investment firm continues to undertake the service itself and therefore falls outside the scope of these rules.



## Relationship with the EBA Guidelines

The MiFID II Delegated Regulation comprises similar provisions to the EBA Guidelines (see page 6). We have compared the relevant provisions from both the MiFID II Delegated Regulation and the EBA Guidelines in Schedule 5 below.

# General Data Protection Regulation (EU) 2016/679

Data has invariably become a fundamental consideration in any outsourcing arrangement. The relevant European framework governing the processing of personal data is the General Data Protection Regulation (EU) 2016/679 (“GDPR”).

## Who does it apply to?

The GDPR has extra-territorial effect and applies to the processing of personal data:

- In the context of an EU establishment;
- In relation to the offerings of goods or services to EU residents; and
- In relation to the monitoring of behaviour of EU residents (to the extent that such behaviour takes place in the EU).

## Timing

The GDPR came into force on 25 May 2018 and aims to harmonise data protection laws across the EU. Given its broad geographic scope and stringent enforcement regime, the GDPR has wide-reaching implications for businesses.

## Scope

The GDPR applies to a company or entity established in the EU which processes personal data, including as part of the activities of one of its branches established in the EU, regardless of where the data is processed. The GDPR also applies to companies established outside the EU that offer goods/services (paid or for free) or are monitoring the behaviour of individuals in the EU.

## Key definitions

- “**controller**” means any person (natural, legal or any other body) that, alone or jointly with others, determines the purposes and means of processing personal data;
- “**data subject**” means an identified or identifiable natural person, and an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person;
- “**personal data**” means data that relates to an identified or identifiable individual (e.g., a name, an identification number, location data or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person);
- “**personal data breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- “**processing**” means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- “**processor**” means any person (natural, legal or other body) processing personal data on behalf of a controller; and
- “**special categories of personal data**” means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

## Internal governance/overarching requirements

In most outsourcing arrangements, organisations that are subject to the GDPR must comply with the broad accountability requirements set out in Article 5 of the GDPR. Organisations are expected to implement a suite of internal processes, procedures, and policies to be able to demonstrate accountability, such as meeting the technical and organisational measures under Article 25 of the GDPR.

Organisations implementing GDPR compliance frameworks should in particular be:

- Documenting a privacy governance model, with clear roles and responsibilities and reporting lines to embed privacy compliance into the organisation;
- *Considering whether a statutory data protection officer or a local EU representative is required;*
- *Developing training for all company personnel;*
- *Reviewing insurance coverage, in light of the higher fines and penalties under the GDPR;*
- *Assessing whether the organisation processes data on a lawful basis, including in relation to any special categories of personal data (often referred to as sensitive personal data);*
- *Putting in place a privacy impact assessment protocol;*

- *Updating privacy policies, including employee-facing privacy policies, and internal processes for managing data subject requests;*
- *Documenting all data processed by the organisation in a detailed record of processing; and*
- *Identifying all cross-border data flows and reviewing data export mechanisms.*

Organisations must also consider the requirements of the GDPR in its dealings with any third parties that may have access to the organisation's data.

## Contractual requirements

Organisations should consider GDPR requirements for any outsourcing arrangement that involves the processing or transfer of data. For example, a number of contractual terms must be put in place between a data controller and data processor pursuant to Article 28 of the GDPR. This particularly requires:

- Ensuring that the processor provides sufficient guarantees regarding the safeguarding of the data;
- Including an obligation on the processor to obtain the specific or general consent of the controller before engaging any subcontractors;
- Setting out the following details:
  - Subject matter and duration of the processing;
  - The nature and purpose of the processing;
  - The type of personal data;
  - Categories of data subjects; and
  - The obligations and rights of the controller.
- Specifying that the processor only processes personal data on the documented instructions and notifies the controller, subject to applicable law;
- Including appropriate confidentiality obligation on the processor, its employees and any subcontractors;
- Detailing security measures the processor shall put in place to safeguard the personal data;
- Imposing appropriate obligations on the processor to cooperate with the controller regarding the rights of data subjects, notify the controller if there is any accidental or unauthorised access to personal data, and providing assistance in such circumstances;
- Placing an obligation on the processor to delete or return all personal data to the controller at the expiration or termination of the agreement; and
- Providing for sufficient audit rights in favour of the controller, e.g., to provide all information necessary to show compliance with data processing obligations.

Notably, if a processor infringes the GDPR by determining the purposes and means of processing, the processor will be considered the controller in respect of such processing.

Where data is being transferred outside of the EEA further contractual requirements may apply. Chapter V of the GDPR requires the controller to ensure a data transfer solution is put in place (e.g., Privacy Shield, Model Clauses, etc.) which ensures the adequate protection of such data when it is transferred to a non-EEA state.

## Application to intra-group/intra-entity arrangements?

### Intra-group arrangements

The GDPR applies to intra-group arrangements. Where intra-group data transfers are taking place in the context of a controller/processor relationship, a data processing agreement incorporating the mandatory clauses set out in Article 28 of the GDPR will regulate the relationship between the group entities and will demonstrate compliance with the GDPR. All data sharing with entities outside of the EEA, even when taking place between group companies, must meet the conditions set forth in Chapter V of the GDPR regarding data export (as described above).

### Intra-entity arrangements

Similar to intra-group arrangements, the GDPR is applicable to intra-entity arrangements and data must be protected to a similar extent. In the event of a branch being outside of the EEA, all data sharing must meet the conditions set forth in Chapter V of the GDPR regarding data export (as described above).



# Directive concerning measures for a high common level of security of network and information systems (EU) 2016/1148

The Directive on Security of Network and Information Systems (EU) 2016/1148 concerning measures for a high common level of security of network and information systems (the “**NIS Directive**”) aims to boost security levels of network and information systems that are considered critical for the provision of digital and essential services.

Please note that directives are not directly applicable in each member state; they require implementation through national legislation in order to have binding legal effect. Accordingly, the application of the NIS Directive across Europe is not harmonised.

## Who does it apply to?

The NIS Directive applies to two groups of organisations: (i) operators of essential services (“**OES**”); and (ii) relevant digital service providers (“**RDSPs**”).

## Timing

The NIS Directive was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. All member states were required to transpose the NIS Directive into national law by 9 May 2018.

## Scope

The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring a culture of security across sectors which are deemed vital for the economy and moreover rely heavily on technology, such as market infrastructures and digital infrastructure. Businesses in these sectors that are identified by Member States as OES have to take appropriate security measures and notify serious incidents to the relevant national authority. RDSPs (including search engines, cloud computing services and online marketplaces) have to comply with security and notification requirements.

## Key definitions

### OES

- “**essential services**” means those that are: (i) critical to the national infrastructure (e.g., water, energy and transport); or (ii) significantly important to the economy and society (e.g., health services and digital infrastructure).
- “**OES**” means: (i) an entity [that] provides a service that is essential for the maintenance of critical societal and/or economic activities; (ii) the provision of that service depends on network and information systems; and (iii) [in this context] an incident would have significant disruptive effects on the provision of that service. An operator of a trading venue such as a regulated market, a multilateral trading facility (“**MTF**”) or an organised trading facility (“**OTF**”) is an example of an OES for the purposes of the NIS Directive (Point 4 of Annex II). Operators of these venues are therefore required to comply with the NIS Directive. Depending on the particular circumstances, operators of these venues may also qualify as an “online marketplace” and therefore a RDSP under the definitions below.

### RDSP

- “**cloud computing service**” means a digital service that enables access to a scalable and elastic pool of shareable computing resources.
- “**online marketplace**” means any digital service that allows consumers or traders to conclude online sales or service contracts with traders either on the online marketplace’s website or on a trader’s website, that uses computing services provided by the online marketplace.
- “**online search engine**” means any digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found.
- “**relevant digital services providers**” means those providing the following services: (i) an online marketplace; (ii) an online search engine; or (iii) a cloud computing service.

Even if an entity is not designated an RDSP or OES, any personal data processing must be compliant with the GDPR and all applicable data privacy legislation.

## Internal governance/overarching requirements

### OES

The NIS Directive states that an OES should take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of its network and information systems (as per Chapter 4, Article 14, NIS Directive). Having regard to the state of the art but not implementation costs, the OES must in its measures ensure a level of security appropriate for the level of risk posed, to prevent and minimise the impact of potential incidents.

An OES is also required to notify, without undue delay, the competent authority or relevant computer security incident response teams (“**CSIRTs**”) of incidents that have a significant impact on the continuity of the essential services the OES provides. Whether an incident has a significant impact is measured by the following factors:

- The number of users affected by the disruption of the essential service;
- The duration of the incident; and
- The geographical spread with regard to the area affected by the incident.

### RDSP

The NIS Directive also states that an RDSP should take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of its network and information systems (as per Chapter 5, Article 16, NIS Directive). An RDSP must, having regard to the state of the art but not implementation costs, ensure a level of security appropriate for the level of risk posed, to prevent and minimise the impact of potential incidents. However, for RDSPs, such measures are additionally expected to cover:

- The security of systems and facilities, including the physical environment of network and information systems;
- Incident handling, such as the procedures for supporting the detection, analysis and containment of an incident;
- Business continuity management, i.e., the ability to maintain or restore the services to appropriate predefined levels;
- Monitoring, auditing, and testing. This includes maintaining policies and processes concerning systems assessment, inspection and verification; and
- Compliance with international standards.

An RDSP must notify the competent authority or the CSIRT, without undue delay, if any incident has a substantial impact on the provision of a service. Whether an incident has a substantial impact is measured by the following factors:

- The number of users affected, in particular users relying on the service for the provision of their own services;
- The duration of the incident;
- The geographical spread with regard to the area affected by the incident;
- The extent of the disruption of the functioning of the service; and
- The extent of the impact on economic and societal activities.

## Contractual requirements

OESs and RDSPs should consider whether any key security obligations may flow down their supply chain. Key suppliers and vendors may hold important data, have access to vital IT infrastructure or help companies maintain appropriate technical and organisational measures. Such third-party contracts should be carefully drafted, with sufficient detail and breadth, to ensure compliance with these requirements. For instance:

- Including broad audit rights to periodically verify that supplier premises are sufficiently secure;
- Contractually managing security performance by key performance indicators, regular reporting, and robust governance mechanisms;
- Limiting onward subcontracting by suppliers to ensure that supply chains remains secure;
- Structuring exit mechanisms that seek to transfer legacy services to new suppliers to ensure that security protections are not diluted; and
- Regularly re-assessing long-term contracts, depending on the level of potential risk, to ensure that security protections do not diminish over time, e.g., as key employees leave.

The UK’s CSIRT (The National Cyber Security Centre) has published guidance<sup>2</sup> on the ways in which an OES should ensure that its supply chain is sufficiently secure. RDSPs should take note of the Commission Implementing Regulation (EU) 2018/151 (“**DSP Regulation**”) which provides additional specific security guidance.

---

<sup>2</sup> National Cyber Security Centre, “Supply chain security guidance”, available at: <<https://www.ncsc.gov.uk/collection/supply-chain-security>>

## Application to intra-group/intra-entity arrangements?

### Intra-group arrangements

The NIS Directive does not specifically refer to intra-group arrangements. Major OESs and RDSPs may segregate different types of data between their various entities, host data in numerous regions or use subsidiaries to maintain different technical and organisational measures. The contractual requirements described above may therefore be as relevant to the intra-group context, with the parent company taking the lead in ensuring consistency and uniformity.

### Intra-entity arrangements

Similarly, the NIS Directive does not specifically refer to intra-entity arrangements. However, for the same reasons as stated for intra-group arrangements the requirements of the NIS Directive may be relevant to an intra-entity arrangement. Therefore, OESs and RDSPs should review their obligations under the NIS Directive if they intend to enter into an intra-entity outsourcing.



## Capital Requirements Directive (2013/36/EU) (“CRD IV”)

Credit institutions and investment firms subject to CRD IV are required to have robust governance arrangements in place, which are comprehensive and proportionate to the nature, scale, and complexity of the risks inherent in the business model and the institution’s activities. Accordingly in-scope entities will need to ensure they consider the impact of any outsourcings that may be relevant to these requirements.

### Who does it apply to?

The relevant provisions apply to credit institutions and investment firms (as defined under MiFID II). For the purposes of CRD IV, a “**credit institution**” means an undertaking, the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account.

### Timing

CRD IV came into force on 1 January 2014.

### Internal governance/overarching requirements

The requirements under Article 74 of CRD IV include:

- A clear organisational structure with well-defined, transparent, and consistent lines of responsibility;
- Effective processes to identify, manage, monitor and report the risks the institution is, or might be, exposed to; and
- Adequate internal control mechanisms including sound administration and accounting procedures and remuneration policies and practices that are consistent with, and promote, sound and effective risk management.

It should be ensured that systems, controls, policies and procedures are in place to identify any outsourcings that may be relevant to these requirements and that appropriate arrangements are put in place, accordingly.

### Application to intra-group/intra-entity arrangements

Any intra-group or intra-entity arrangements that impact any of the requirements under CRD IV should be taken into account in the same way as for third party outsourcings. This would include outsourcings to a branch of a legal entity.



# Money Laundering Directive (EU) 2015/849 (“MLD”)

Credit institutions and investment firms subject to the MLD will remain responsible for the performance of their obligations under the MLD regardless of whether they have outsourced certain functions to a third party. Consequently, applicable credit institutions and investment firms need to have provisions in place with third-party service providers that allow firms to satisfy their obligations under the MLD.

## Who does it apply to?

- The relevant provisions apply to credit institutions (as defined in relation to CRD IV, above) and financial institutions. For the purposes of the MLD, a “**financial institution**” means:
  - An undertaking other than a credit institution, which carries out one or more of the activities listed in points (2) to (12), (14) and (15) of Annex I to CRD IV, including the activities of currency exchange offices;
  - An insurance undertaking as defined in point (1) of Article 13 of Solvency II, insofar as it carries out life assurance activities covered by that Directive;
  - An investment firm (as defined under MiFID II);
  - A collective investment undertaking marketing its units or shares;
  - An insurance intermediary (i.e., any natural or legal person who, for remuneration, takes up or pursues insurance mediation) where it acts with respect to life insurance and other investment-related services, with the exception of a tied insurance intermediary as defined in point of that Article; or
  - Branches, when located in the EU, of financial institutions as referred to in points (i) to (v), whether their head office is situated in an EU Member State or in a third country.

## Timing

The MLD entered into force on 26 June 2017.

The MLD has been updated by The Fifth Money Laundering Directive ((EU) 2018/843) (“**MLD5**”), which Member States were required to transpose by 10 January 2020; however, this is unlikely to impact any of the provisions of the MLD discussed in this section.

## Internal governance/overarching requirements

Firms subject to the MLD are required to undertake certain due diligence measures, as outlined at Article 13(1) of the MLD:

- Identify the customer and verify the customer’s identity on the basis of documents, data, or information obtained from a reliable and independent source;
- Identify the beneficial owner and take reasonable measures to verify that person’s identity, so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations, and similar legal arrangements, taking measures to understand the ownership and control structure of the customer;
- Assess, and as appropriate obtain information on the purposes and intended nature of the business relationship; and
- Conduct ongoing monitoring of the business relationship including scrutiny of transactions undertaken through the course of that relationship to ensure that the transactions being conducted are consistent with the firm’s knowledge of the customer, the business and risk profile including where, if necessary, the source of the funds, and ensure that the documents, data, or information are kept up to date.

Should a financial institution decide to outsource any of the functions stated above, it must note the following:

- Although financial institutions may rely on third parties (as defined in Article 26(1) of the MLD) to meet these requirements, the ultimate responsibility for their performance rests with the delegating financial institution;
- Financial institutions may not rely on, or outsource to, third parties established in high-risk third countries;
- Financial institutions must ensure they obtain from the third party to whom they have outsourced all of the information relied on above; and
- In the event of an outsourcing of any of the above functions, the financial institution must ensure that appropriate arrangements are in place to ensure the performance and on-going monitoring of such functions.

Note, the MLD states that the provisions relating to reliance on third parties to meet the customer due diligence requirements do not apply to outsourcing or agency relationships whereby the outsourcing service provider is regarded to be part of the firm itself.



## Application to intra-group/intra-entity arrangements

### Intra-group arrangements

A firm cannot delegate responsibility for completing identity checks under the MLD in an intra-group arrangement, though the firm can delegate the task. Therefore, a firm should be aware of the requirements of the MLD when entering such arrangements.

### Intra-entity arrangements

In an intra-entity arrangement both the fulfilment of, and responsibility for, the MLD requirements fall on the firm in question. Therefore, the outsourcing requirements of the MLD are not directly applicable to intra-entity arrangements.

# Benchmarks Regulation (EU) (2016/1011) (“BMR”)

Benchmark administrators must ensure ongoing compliance with certain BMR provisions when outsourcing certain functions.

## Who does it apply to?

Benchmark administrators. Under the BMR, a “**benchmark administrator**” means “a natural or legal person that has control over the provision of a benchmark”.

## Timing

BMR entered into force for all new benchmarks from 1 January 2018. The transition period for BMR ends on 1 January 2020, at which point BMR shall apply to all benchmarks.

## Scope

Benchmark administrators subject to the BMR may not outsource functions in the provision of a benchmark in such a way as to impair materially the benchmark administrator’s control over the provision of the benchmark, or the ability of the relevant competent authority to supervise the benchmark. Further, where a benchmark administrator outsources to a service provider functions or any relevant services and activities in the provision of a benchmark, the benchmark administrator shall remain fully responsible for discharging all of the benchmark administrator’s obligations under the BMR.

## Internal governance/overarching requirements

The requirements under Article 10 of the BMR, include:

- Where there is outsourcing, the benchmark administrator must ensure that the following obligations are complied with:
  - The service provider has the ability, capacity, and any authorisation required by law, to perform the outsourced functions, services or activities reliably and professionally;
  - The benchmark administrator makes available to the relevant competent authorities the identity and the tasks of the service provider that participates in the benchmarks determination process;
  - The benchmark administrator takes appropriate action if it appears that the service provider may not be carrying out the outsourced functions effectively and in compliance with applicable law and regulatory requirements;
  - The benchmark administrator retains the necessary expertise to supervise the outsourced functions effectively and to manage the risks associated with the outsourcing;
  - The service provider discloses to the benchmark administrator any development that may have a material impact on its ability to carry out the outsourced functions effectively and in compliance with applicable law and regulatory requirements;
  - The service provider cooperates with the relevant competent authority regarding the outsourced activities, the benchmark administrator and the relevant competent authority have effective access to data related to the outsourced activities and to the business premises of the service provider, and the relevant competent authority is able to exercise those rights of access;
  - The benchmark administrator is able to terminate the outsourcing arrangements where necessary; and
  - The benchmark administrator takes reasonable steps, including contingency plans, to avoid undue operational risk related to the participation of the service provider in the benchmark determination process.

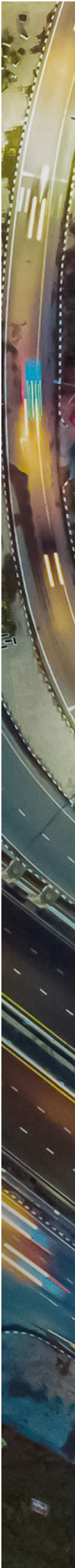
## Application to intra-group/intra-entity arrangements

### Intra-group arrangements

These requirements apply to intra-group arrangements and therefore the above should be followed. Note, the benchmark administrator shall remain fully responsible for discharging all of the benchmark administrator’s obligations under the BMR.

### Intra-entity arrangements

In an intra-entity arrangement both the fulfilment of, and responsibility for, the BMR requirements fall on the firm in question. Therefore, the outsourcing provisions of the BMR are not directly applicable.



# ESMA GUIDELINES ON CERTAIN ASPECTS OF MIFID COMPLIANCE FUNCTION REQUIREMENTS (28 SEPTEMBER 2012 (UPDATED 5 JUNE 2020)) (2012/388) (THE “ESMA GUIDELINES”)

The ESMA Guidelines set out certain requirements that must be complied with where the compliance function, required under Article 6 of MiFID Implementing Directive 2006/73/EC (“**MiFID Implementing Directive**”), is outsourced to other firms.

## Who does it apply to?

Investment firms, credit institutions that provide investment services, UCITS management companies, and competent authorities as defined under MiFID II.

## Timing

The ESMA Guidelines were published on 28 September 2012 and were updated on 5 June 2020.

## Scope

The ESMA Guidelines are relevant where all or part of the compliance function is outsourced.

## Internal governance/overarching requirements

The relevant guidance under the ESMA Guidelines includes the following:

- Investment firms should ensure that all applicable compliance function requirements are fulfilled where all or part of the compliance function is outsourced. The responsibility for the fulfilment of the existing requirements rests with the investment firm’s senior management;
- The investment firm should conduct a risk assessment to ensure that compliance risks are comprehensively monitored;
- The investment firm should ensure that the service provider has the necessary authority, resources, expertise, and access to all relevant information in order to perform the outsourced compliance function tasks effectively;
- The investment firm should favour an organisation where control functions are properly segregated (the combination of the compliance function with other control functions may be acceptable if this does not compromise the effectiveness and independence of the compliance function);
- Investment firms should ensure that, when outsourced partially or fully, the compliance function remains permanent, independent and effective in nature (i.e., the service provider should be able to perform the function on an ongoing basis and not only in specific circumstances even if the compliance officer is absent);
- Investment firms should monitor whether the service provider performs its duties adequately (including, monitoring the quality and the quantity of the services provided via a risk-based monitoring programme that evaluates whether the firm’s business is conducted in compliance with its obligations under MiFID II);
- Investment firms should prepare mandatory compliance reports that cover all business units involved in the provision of investment services, activities and ancillary services provided by the firm;
- Investment firms should take into account the scale and types of investment services, activities and ancillary activities undertaken by the firm;
- Investment firms should make sure that their compliance staff have the necessary skills, knowledge and expertise to discharge their responsibilities under MiFID;
- While the outsourcing of the compliance function within a group does not lead to a lower level of responsibility for the senior management of the individual investment firms within the group, a centralised group compliance function may, in some cases, provide the compliance office with better access to information and lead to greater efficiency of the function (especially if the entities share the same premises); and
- If an investment firm, due to the nature, size and scope of its business activities, is unable to employ compliance staff who are independent of the performance of the services they monitor, then outsourcing of the compliance function is likely to be an appropriate approach to take.



## Application to intra-group/intra-entity arrangements

### Intra-group arrangements

The guidelines set out above should be followed where the arrangement is intra-group. The ESMA Guidelines state that to the extent that the investment firm and the service provider are members of the same group, the investment firm may take into account the extent to which it controls the service provider or has the ability to influence its actions.

### Intra-entity arrangements

In an intra-entity arrangement both the fulfilment of, and responsibility for, the compliance function of a firm will fall upon the firm in question. Therefore, the outsourcing provisions of the ESMA Guidelines are not directly applicable.

## Outsourcing post-brexit: EBA and ECB guidance

The EBA and the ECB have noted that in the course of the United Kingdom's withdrawal from the European Union, UK-based market participants may seek to relocate entities, activities or functions to the EU in order to retain market access. In this process, firms may seek to minimise the transfer of the effective performance of those activities or functions to the EU by relying on the outsourcing or delegation of activities to UK-based entities or affiliates. Both the EBA and ECB's guidance distinguish between "third country entities" and "third country branches" and consequently apply to both intra-group and intra-entity outsourcings. The EBA and the ECB are therefore concerned to ensure that the conditions for outsourcing and delegation do not generate supervisory arbitrage risks. As a result, the EBA and the ECB have issued guidance to ensure that the Brexit process does not result in the development of 'letter-box entities' in the EU, and that outsourcing to third countries (including the UK) only occurs under strict conditions.

### Opinion of the European Banking Authority on the issues related to the departure of the United Kingdom from the European Union

On 12 October 2017, the EBA issued an opinion<sup>3</sup> on issues related to the departure of the United Kingdom from the European Union (the "EBA Opinion"). The EBA Opinion sets out key principles in relation to the impact of Brexit on internal governance, outsourcing, risk transfers and 'empty shell companies', affirming the need for entities outsourcing to third countries to maintain effective systems of governance and control, and the ability to manage risk within the EU entity. These principles are:

- Institutions should have sound and effective governance and suitable members of the managing body;
- Institutions should not outsource activities to such an extent that they operate as 'empty shell' companies, and all institutions should have the resources and ability to identify and manage the risks they generate;
- Risk management is an important function of credit institutions and investment firms which goes hand in hand with the extension of business. Local risk management needs to be commensurate to the business extended. With respect to outsourcing, institutions should be able to monitor and manage the outsourcing arrangements, and ensure that authorities have full access to all information they need to fulfil their supervisory function;
- EU27 authorities should have regard to the fact that after Brexit the UK will be a third country and thus activities outsourced to institutions in the UK prior to Brexit should be assessed with regard to the ability of the institution to adapt to this possible scenario;
- Institutions engaging in back-to-back or intra-group operations to transfer risk to another entity should have adequate resources to identify and fully manage their counterparty credit risk, and any material risks that they have transferred in the event of the failure of their counterparty; and
- Institutions should demonstrate their ability to continuously access financial market infrastructures (located in the UK), and assess any impact from losing continued access to such infrastructures. Institutions' risk management and governance should be scalable in times of crisis and the local capabilities should ensure that risks could be managed or, if needed, positions could be unwound in an orderly way.

The EBA Opinion sets out EBA's expectations on NCAs for the purposes of fulfilling its principles. In particular, it reminds NCAs that any outsourcing or delegation arrangement from entities authorised in the EU27 to third country entities should be strictly framed and constantly supervised. In addition, outsourcing or delegation arrangements under which entities confer either a substantial degree of activities or critical functions to other entities, should not result in those entities becoming 'letterbox' entities, nor in creating obstacles to effective and efficient supervision and enforcement.

### ECB Supervisory Expectation on Booking Models

In August 2018 the ECB published supervisory expectations (the "ECB Expectations")<sup>4</sup> regarding the assessment of booking models on risk management and governance in order to take into account the EBA Opinion. The ECB expectations introduce the views of ECB banking supervision on empty shells and booking models. In particular, the ECB Expectations focus on the risk framework from a first/second line perspective, covering five areas:

- Internal governance, staffing and organisation:
  - Firms should put in place a robust governance and risk management framework, including related documentation. Firms should be adequately staffed and include sufficient knowledge, experience, capabilities and technology to manage both the existing and relocating business and associated risks; and
  - Firms' management bodies should have a clear understanding of all risks, and effective control over the entity's balance sheet.

<sup>3</sup> EBA, 12 October 2017, "Opinion of the European Banking Authority on issues related to the departure of the United Kingdom from the European Union", available at: <https://eba.europa.eu/sites/default/documents/files/documents/10180/1756362/81e612c6-dcab-4c4b-87e9-32784cb44de1/EBA%20Opinion%20on%20Brexit%20Issues%20%28EBA-Op-2017-12%29.pdf?retry=1>

<sup>4</sup> European Central Bank, August 2018, "Supervisory Expectations on booking models", available at: [https://www.bankingsupervision.europa.eu/banking/relocating/shared/pdf/ssm\\_supervisorexpectationsbookingmodels\\_201808\\_en.pdf](https://www.bankingsupervision.europa.eu/banking/relocating/shared/pdf/ssm_supervisorexpectationsbookingmodels_201808_en.pdf)

- Business origination and FMI access:
  - Firms should not have a heavy reliance on third country risk hubs. As such, firms are expected to manage their market and counterparty risk independently and have independent trading capability, as well as diversified counterparties within the EU27; and
  - When firms access FMIs via a third country entity or branch, they should consider which alternative FMIs are available in the event that their access to third country FMIs is lost or no longer guaranteed.
- Booking and hedging strategy:
  - Firms should maintain sufficient independence by safeguarding local decision making capacities, and retaining control over the balance sheet; and
  - Entities should identify clearly their hedging strategies, procedures, controls and governance in a booking model policy.
- Intra-group arrangements:
  - Firms making intra-group arrangements should avoid undue complexity, for example, through legal entity structures or hedging measures; and
  - Firms should retain the ability independently to monitor and manage risks arising from intra-group exposures.
- IT infrastructure and reporting:
  - Firms should retain the ability to produce daily complete and accurate reports;
  - IT infrastructure should be commensurate with the firm's transfer of assets/business; and
  - In a crisis, operational continuity and access to necessary operational assets should be ensured via adequate contractual provisions (e.g., SLA) and business continuity plans.

The ECB notes that the ECB Expectations on booking models and empty shells will be applied in a proportionate manner to individual cases, taking into account the materiality and complexity of the firm's capital market activities.

# THE REVISED PAYMENT SERVICES DIRECTIVE (EU) 2015/2366

The Revised Payment Services Directive (EU) 2015/2366 (“PSD2”) incorporated and repealed the Payment Services Directive (2007/64/EC) with the aim of modernising the regulatory framework to account for new types of payment services.

## Who does it apply to?

PSD2 applies to all payment services providers including (but not limited to) payment institutions, credit institutions, e-money institutions, central banks and governments.

## Timing

PSD2 was published on 23 December 2015, entered into force on 12 January 2016 and had to be transposed into national law by Member States by 13 January 2018.

## Scope

PSD2 provides the legal foundation for an EU single market for payments, to establish safer and more innovative payment services across the EU.

## Internal governance/overarching requirements

Outsourcing of payment services is addressed by Article 19 of PSD2, which is summarised as follows:

- Where a payment institution intends to provide payment services through an agent it shall communicate the following information to the competent authorities of its home Member State:
  - Name and address of agent;
  - A description of the internal control mechanisms that will be used by the agent to ensure compliance with AML and ATF laws;
  - The identity of the directors and persons responsible for the management of the agent (including evidence that they are fit and proper persons);
  - The payment services of the payment institution for which the agent is mandated; and
  - Where applicable, the unique identification code or number of the agent,
- Within two months of receipt of the above information, the competent authority will communicate to the payment institution whether the agent has been entered in the register (as stipulated by Article 14 of PSD2);
- If the payment institution wishes to provide payment services in another Member State by engaging an agent or establishing a branch it shall follow the procedures set out in Article 28 of PSD2 (materially similar to the information provided above);
- Where a payment institution intends to outsource operational functions of payment services, it shall inform the competent authorities of its home Member State accordingly (namely, that outsourcing of important<sup>5</sup> operational functions (including IT systems), shall not be undertaken in a manner that impairs the quality of the payment institution’s internal control or the ability of the competent authorities to monitor and retrace compliance);
- Payment institutions shall ensure that agents and branches acting on their behalf inform users of this fact; and
- Any changes to the entities whose activities are outsourced to must be communicated to the competent authorities of the payment institution’s home Member State.

Under Article 20 of PSD2, a payment institution remains fully liable for any acts of any agent, branch or entity to which activities are outsourced.

## Application to intra-group/intra-entity arrangements

### Intra-group arrangements

These requirements apply to intra-group arrangements and therefore the above should be followed. Note, under PSD2 the outsourcing entity shall remain fully responsible for discharging all of its obligations under PSD2.

### Intra-entity arrangements

The requirements apply to intra-entity arrangements, with branches being specifically considered in the outsourcing provisions and defined as “a place of business other than the head office which is a part of a payment institution, (and) which has no legal personality”.

<sup>5</sup> An operational function shall be regarded as important if a defect or failure in its performance would materially impair the continuing compliance of a payment institution with the requirements of its authorisation.



# PART THREE

## JURISDICTION SPECIFIC GUIDANCE

---

Part Three highlights the areas where local law and/or the local regulatory position adopted by financial services regulators materially differs from the macro-level European position, as defined in Parts One and Two. The default position for each of the below jurisdictions is the position detailed in Parts One and Two of this Paper, and is only different where stated below. The jurisdictions covered within this section include:

- France;
- Germany;
- Ireland;
- Italy;
- Luxembourg;
- Spain; and
- UK

# France

## Regulatory approach

The French Prudential Control Authority, Autorité de contrôle prudentiel et de résolution (the “ACPR”), the supervisory authority with an overall view of the banking, financial and insurance sectors, has been interested in the issue of outsourcing since before any specific law or regulation was implemented in this area. In 2004, the ACPR released a study on outsourcing for financial services in France, partially based on the guidelines of the Committee of European Banking Supervisors (the “CEBS”) which raised 11 “High Level Principles” setting out what supervisory authorities should expect from institutions. This study identified the main: (i) outsourcing strategies adopted by French credit institutions (i.e., intra-group outsourcings and/or use of French non-financial (or regulated) entities); and (ii) risks relating to outsourcing (for example, operational risks such as the risk of operational disruption resulting in harm to clients and risks relating to the loss of control over certain outsourced activities).

The regulation of outsourcing for financial services has been led by European regulations and directives, which have been implemented in France primarily by Law No. 2013-672 of 26 July 2013 on the Separation and Regulation of Banking Activities, and the order of 3 November 2014 on internal control of companies in the banking, payment services and investment services sectors subject to ACPR supervision (the “**Order of 3 November 2014**”), as amended from time to time.

Note, that the obligations and regulatory requirements of French insurance companies relating to outsourcing have been excluded from this analysis.

## ACPR Notice on outsourcing (the “ACPR Notice”)

The ACPR often issues notices to explain to regulated entities how a particular regulation will be implemented, however, said notices do not necessarily answer all the questions raised by such implementation.

On 15 July 2019, the ACPR published a notice on the EBA Guidelines, in which the ACPR stated its intention to fully comply with the EBA Guidelines on outsourcing.

All French financial institutions that are within the scope of the EBA Guidelines are expected to comply with the EBA Guidelines (i.e., financial institutions that are within the scope of the EBA’s mandate, including credit institutions, investment firms subject to CRD IV, payment institutions and electronic money institutions). Moreover, the ACPR decided to extend the scope of the EBA Guidelines to French finance companies, and companies that are authorised by the ACPR, such as credit institutions whose business is limited to credit granting (it being specified that such credit institutions do not carry out the business of taking deposits or other repayable funds from the public).

This ACPR Notice came into force on 30 September 2019, at the same time as the entry into force of the EBA Guidelines.

The EBA Guidelines apply to French financial institutions in accordance with the rules relating to outsourcing which are set out in the Order of 3 November 2014. Please note, no changes were made to existing French regulation on outsourcing following the publication of the EBA Guidelines.

## Order of 3 November 2014 – Internal control

The Order of 3 November 2014 replaces the former regulations applicable to the internal control of regulated entities subject to ACPR supervision by adapting them to the European definitions and regulations.

Under the Order of 3 November 2014, regulated entities subject to ACPR supervision must comply with rules regarding compliance, governance, anti-money laundering and terrorist financing, monitoring and management of risks, in relation to outsourcing.

### Definitions

The Order of 3 November 2014 does not use the definition of outsourcing set out in the EBA Guidelines or the MiFID II Delegated Regulation, rather:

- “**outsourced activities**” are defined as activities for which the outsourcing entity entrusts to a third party, on a long-term basis and on a regular basis, the performance of critical or important operational services or tasks by sub-contracting within the meaning of Law No. 75-1334 of 31 December 1975, a French law adopted in order to guarantee the rights of the sub-contractor, or by other means listed in the Order of 3 November 2014.

The definition of the critical or important functions within the meaning of the Order of 3 November 2014 is similar to the definition given in the MiFID II Delegated Regulation and the EBA Guidelines:

- “**critical or important operational services or tasks**” are those listed in the Order of 3 November 2014, corresponding to the core business of the outsourcing entity, and to any service or task where a defect or failure in its performance would materially impair the continuing compliance of an outsourcing entity with the conditions and obligations of its authorisation or its other obligations under MiFID II, or its financial

performance, or the soundness or the continuity of its investment services and activities. Without prejudice to the status of any other service or task, the following services or tasks shall not be considered critical or important:

- the provision of advisory services, and other services which do not form part of the core business of the institution (including legal advice, training of personnel, billing services and the security of the institution's premises and personnel);
- the purchase of standard services, including market information services and the provision of price feeds.

### Who does it apply to?

The Order of 3 November 2014 applies to:

- Credit institutions;
- Finance companies;
- Investment firms;
- Payment institutions; and
- Electronic money institutions.

### Internal governance/overarching requirements

The requirements set out in the Order of 3 November 2014 are similar to the requirements set out in the MiFID Delegated Regulation, though the scope of application of the Order of 3 November 2014 is broader than: (i) the MiFID Delegated Regulation (which only applies to investment firms), and (ii) the requirements set out in the EBA Guidelines, except subject, inter alia, to the specified following rules:

- The practical application of the requirements such as the outsourcing policy and the outsourcing register provided for in the EBA Guidelines; and
- Under the MiFID Delegated Regulation, the sub-outsourcing by the service provider shall only take place with the consent, in writing of the investment firm.

Despite the above two points not being provided by French regulation, outsourcing entities must still comply with them (in accordance with the ACPR Notice and the direct effect of European regulation).

### Relationships with the ACPR

Under Article 232 of the Order of 3 November 2014, prior notification to the ACPR is required when an operational function of payment services or of issuing and managing electronic money is outsourced by payment institutions, account information service providers or electronic money institutions. This notification requirement is provided under the French Monetary and Financial Code, which indicates that the outsourcing of important operational functions shall not impair the quality of the internal control of the institution and shall not impair the ACPR's ability to monitor the institution's compliance.

### Restrictions on outsourcing

Under Article 231 of the Order of 3 November 2014, an outsourcing entity may only outsource the following activities to authorised entities:

- Banking operations, issuance and management of electronic money, payment services and investment services for which the institution has been authorised;
- Certain related services; and
- Any service directly involved in the performance of the services listed above.

### Contractual requirements

As provided under the MiFID Delegated Regulation, and the Order of 3 November 2014, outsourcing arrangements must be in writing and contain provisions on data security, audit rights and business continuity plan.

### Application to intra-group/intra-entity arrangements

Outsourcing agreements may be entered into between intra-group companies. The provisions of the Order of 3 November 2014 on outsourcing apply in the context of intra-group arrangements, however, to the extent that the institution and the service provider are members of the same group, the institution may take into account the extent to which the institution controls the service provider or the ability to influence its actions.

## The AMF General Regulation

The Order of 3 November 2014 excludes from its scope asset management companies, as these entities are subject to the rules set forth by the French Financial Markets Authority, Autorité des marchés financiers (the "AMF"), the public authority responsible for ensuring that savings invested in financial products are protected.

The general regulation of the AMF (the "AMF General Regulation") has introduced requirements relating to outsourcing which are in line with the EBA Guidelines and the obligations set forth under the Order of 3 November 2014, save for specific requirements described below.

## Definitions

- “outsourcing” has the same meaning as in the EBA Guidelines.
- “critical operational tasks and functions or tasks and functions that are important” (the “critical or important tasks and functions”), has a similar definition to that provided in the Order of 3 November 2014; that a task/function shall be regarded as critical or important if a defect or failure in its performance would materially impair the asset management company’s capacity for continuing compliance with the conditions and obligations of its authorisation or its professional obligations referred to in the relevant provisions of the French Monetary and Financial Code, its financial performance, or the continuity of its business. Without prejudice to the status of any other task or function, the following tasks or functions shall not be considered as critical or important:
  - the provision of advisory services, and other services which do not form part of the investment services of the firm (including legal advice, training of personnel, billing services and the security of the asset management company’s premises and personnel); and
  - the purchase of standard services, including market information services and the provision of price feeds.

## Who does it apply to?

The AMF provisions on outsourcing are applicable to: (i) collective investment in transferable securities (“UCITS”); and (ii) alternative investment fund managers (“AIFMs”), as these terms are respectively defined by Directive 2009/65/EC on the coordination of laws, regulations and administrative provisions relating to undertakings for UCITS and Directive 2011/61/EU on AIFMs, (the “asset management company”).

## General requirements

While outsourcing the execution of critical or important tasks and functions for the provision of a service, asset management companies shall:

- Take all reasonable measures to prevent an undue exacerbation of operating risk;
- Not outsource in such a way that it materially impairs the quality of internal control and prevents the AMF from verifying that the asset management companies comply with all their obligations; and
- Not outsource to an extent that turns the asset management companies into “letter box entities”, which would be deemed a breach of their obligations relating to the obtaining and maintenance of their regulatory authorisations.

## Internal/Governance obligations

Asset management companies that outsource critical or important tasks and functions shall remain fully responsible for complying with all their professional obligations as set forth under the relevant provisions of the French Monetary and Financial Code, complying in particular with the following conditions:

- Outsourcing must not result in the delegation by senior management of its responsibility;
- The relationship and obligations of the asset management companies towards its clients must not be altered; and
- The conditions or commitments with which the asset management companies must comply in order to be authorised must not be undermined.

## Contractual requirements

As provided in the MiFID Delegated Regulation and the Order of 3 November 2014, outsourcing arrangements must be in writing and shall contain provisions on data security, audit rights and business continuity plans.

When entering into, managing or terminating outsourcing arrangements, asset management companies shall exercise due skill, care and diligence. In particular, asset management companies must take the necessary steps to ensure that the following conditions are satisfied:

- *Conditions to be met by the service provider:*
  - The service provider must have the ability, capacity, and any authorisation required to perform the outsourced tasks or functions reliably and professionally;
  - The service provider must carry out the outsourced services effectively. To this end, the asset management company must establish methods for assessing the standard of performance of the service provider;
  - The service provider must properly supervise the carrying out of the outsourced tasks or functions, and adequately manage the risks stemming from outsourcing;
  - The service provider must disclose to the asset management company any development that may have a material impact on its ability to carry out the outsourced tasks or functions effectively and in compliance with the professional obligations referred to in the relevant provisions of the French Monetary and Financial Code applying to them;
  - The service provider must cooperate with the AMF in connection with the outsourced tasks or functions; and



- The service provider must protect any confidential information relating to the asset management company and its clients.
- *Conditions to be met by asset management companies:*
  - Asset management companies must take appropriate action if it appears that the service provider may not be carrying out the functions effectively and in compliance with the professional obligations referred to in the relevant provisions of the French Monetary and Financial Code applying to them;
  - Asset management companies must retain the necessary expertise to supervise the outsourced tasks or functions effectively and manage the risks stemming from outsourcing and must supervise those tasks and manage those risks; and
  - Asset management companies, their auditors and the relevant competent authorities must have effective access to data related to the outsourced tasks or functions, as well as to the business premises of the service provider.
- *Conditions applying to both asset management companies and the service provider:*
  - Establish and maintain an effective contingency plan for disaster recovery and periodic testing of backup facilities, where that is necessary having regard to the nature of the outsourced task or function; and
  - The procedures for terminating outsourcing contracts at the initiative of either party must ensure the continuity and the quality of the activities carried out.

### Application to intra-group/intra-entity arrangements

Where the asset management company and the service provider are members of the same group or are under the same central body, the asset management company may, for the purposes of determining how the requirements described above shall apply, take into account the extent to which it controls the service provider or has the ability to influence its actions.

### Outsourcing to a service provider located outside the EEA

In this case, as provided under the MiFID II Delegated Regulation, asset management companies must ensure that the following conditions are satisfied:

- The service provider must be authorised or registered in its home country to provide portfolio management service for third parties and it must be subject to prudential supervision; and
- There must be an appropriate cooperation agreement between the AMF and the competent authority of the service provider.

In the case of portfolio management for a retail client, if one or both of the conditions referred to above are not satisfied, asset management companies may outsource portfolio management services to a service provider located in a State that is not party to the EEA, but only if it notifies the AMF about the outsourcing arrangement. In the absence of any observations by the AMF within three months of the notice being given, the planned outsourcing by the asset management companies may be implemented.

## Enforcement

Neither the ACPR nor the AMF provide for specific sanctions applied to non-compliance with outsourcing requirements. The sanctions described below refer to the general enforcement powers of each authority.

### Enforcement by the ACPR

The ACPR is empowered to carry out on-site inspections and investigations. It may take administrative measures such as providing:

- A cautionary note whereby the ACPR warns the relevant institution against continuing practices that may compromise the interests of its clients as they are contrary to the rules of good practice of the profession concerned; and/or
- A formal notice to take, within a specified period of time, any measures intended to bring the relevant institution into compliance with the applicable obligations.

The relevant institutions may be subject to the following sanctions:

- A warning;
- An admonishment;
- A prohibition against carrying out certain transactions for up to ten years;
- Temporary suspension of management for up to ten years;
- The dismissal of management;
- Partial or total withdrawal of approval or authorisation;
- Removal from the list of authorised persons/institutions; and/or
- Fines to a maximum value of EUR 100,000,000.



**The ACPR is also entitled to:**

- Communicate to the public any information deemed necessary for the accomplishment of its missions;
- Publish its sanctions; and
- Modify or withdraw any document contrary to any applicable law and/or regulation.

Sanctions inflicted by the ACPR may be challenged in court.

**Enforcement by the AMF**

The AMF is empowered to carry out: (i) investigations; (ii) off-site examinations of records; and (iii) on-site inspections at the business premises of the entities and/or persons subject to the rules and obligations set forth under the French Monetary and Financial Code and the AMF general regulation.

The AMF is entitled to issue the following sanctions:

- A warning;
- An admonishment;
- A temporary or permanent suspension to exercise all or part of the services provided; and
- Fines to a maximum value of EUR 100,000,000 or ten times the amount of the benefit deriving from the failure to fulfil obligations, if such benefit can be determined.

Sanctions inflicted by the AMF may be challenged in court.

# Germany

## Overview of regulatory framework

The regulatory framework for outsourcing in Germany is set out in German law and supplemented by guidance from the German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht, “**BaFin**”). This framework partially overlaps with the directly applicable EU outsourcing rules and EU guidance and therefore each must be read in conjunction with the other.

### Applicability of EBA Guidelines on outsourcing

While BaFin has not yet implemented the EBA Guidelines on outsourcing, it has announced that it intends to implement the guidelines in the first quarter of 2021 in a revised version of its so-called Minimum Requirements for Risk Management (Mindestanforderungen an das Risikomanagement, “**MaRisk**”). Until such date, the EBA Guidelines will not be applicable to less significant German institutions or other German institutions. With regards to significant German institutions subject to ECB supervision, the ECB has announced that it will apply the EBA Guidelines on outsourcing for the 2020 Supervisory Review and Evaluation Process (SREP).

The following overview of the current regulatory framework in Germany therefore does not comprise any amendments to BaFin’s guidance due to the implementation of the EBA Guidelines, as BaFin has not yet published a consultation draft of the revised MaRisk.

### The key German legal provisions and guidance on outsourcing by credit institutions and/or investment firms are:

**Section 25b German Banking Act** (Kreditwesengesetz, “**KWG**”): Section 25b of the KWG is a general provision on requirements related to outsourcing by credit institutions and investment firms (together “**financial institutions**”). Broadly, where a financial institution outsources “critical functions”, it requires the implementation of adequate measures to prevent undue risk and an effective risk management framework.

**Section 80(6) German Securities Trading Act** (Wertpapierhandelsgesetz, “**WpHG**”): Section 80(6) of the WpHG provides that any outsourcing by an investment firm must not: (i) alter the legal relationship between the firm and its clients or its obligations towards clients; or (ii) affect the conditions on which the firm’s regulatory licence pursuant to Section 32 of the KWG is based.

**Chapter AT 9 MaRisk:** The general requirements in section 25b of the KWG and section 80(6) of the WpHG are substantiated in more detail in chapter AT 9 of the MaRisk. The MaRisk is a set of administrative rules issued by BaFin in the form of a circular and updated from time to time. The most recent version is Circular 9/2017 dated 27 October 2017, and it is supplemented by an annex with further comments by BaFin (Erläuterungen zu den MaRisk in der Fassung vom 27.10.2017). The MaRisk does not specifically address EU outsourcing rules, but generally sets out requirements regarding the risk management of financial institutions, including those in relation to outsourcing. The MaRisk is not law and thus, strictly speaking, is not binding on financial institutions. However, it reflects BaFin’s administrative practice and thus is widely considered and followed by financial institutions as a quasi-statutory regulation. The MaRisk follows a principles-based approach, which means that its requirements do not apply rigidly or in all cases, but are instead guidelines to be considered by financial institutions to determine which measures should be taken in light of the actual risk related to the outsourcing.

**BAIT:** The Supervisory Requirements for IT in Financial Institutions (Bankaufsichtliche Anforderungen an die IT, “**BAIT**”) issued by BaFin provide further (non-exhaustive) guidelines and requirements regarding the management of IT resources and IT risk management of financial institutions in general, supplementing the requirements set out in the MaRisk. The BAIT are not specifically related to outsourcing but do contain a section on outsourcing that mostly deals with outsourcing of non-critical IT functions including the use of cloud services.

**BaFin Cloud Guidance:** BaFin published guidance on outsourcing to cloud service providers (the “**BaFin Cloud Guidance**”) in late 2018. The BaFin Cloud Guidance can be understood as a specification of the requirements set out in section 25b KWG and chapter AT 9 of the MaRisk with the aim of addressing the specific negative developments which BaFin has come across, for example limitations on or even exclusions of audit and instruction rights provided in the agreements of cloud service providers with customers from the financial industry. The BaFin Cloud Guidance makes clear that the regulatory requirements regarding outsourcing of critical functions fully apply to outsourcing to cloud service providers if it is categorized by the financial institution as an outsourcing of critical functions. While the BaFin Cloud Guidance expressly states that it does not create any new requirements and only reflects the current administrative practice of BaFin, it appears to go beyond the requirements set out in the MaRisk in some respects.

**Section 17 German Anti-Money Laundering Act:** The German Anti-Money Laundering Act (Geldwäschegesetz, “**GwG**”), which transposes MLD/MLD5 into German law, contains certain provisions regarding the performance of AML related activities by third parties. The rules differentiate between: (i) the performance of client due diligence obligations by certain qualified third parties; and (ii) the outsourcing of the client due diligence obligations to other third parties.

**Chapter BT 1.3.4 MaComp:** Chapter BT 1.3.4 of BaFin Circular 05/2018 – Minimum Requirement for Compliance Requirements and restrictions regarding the outsourcing of compliance function and compliance activities

(Mindestanforderungen an die Compliance-Funktion, “**MaComp**”) provides for certain requirements specifically relating to outsourcing of compliance functions or compliance activities.

### In the broader financial services context, further legal provisions and guidance on outsourcing apply to:

**UCITS managers and AIF managers:** The requirements regarding outsourcing by UCITS and AIF managers are set out in Article 13 of the UCITS Directive (Directive 2009/65/EC) and Article 20 of the AIFM Directive (Directive 2011/61/EU) as transposed into German law by Section 36 of the German Capital Investment Code (Kapitalanlagegesetzbuch). They are further specified in sections 75 through 82 of the Commission Delegated Regulation (EU) No 231/2013, the BaFin Circular 01/2017 (WA) dated 10 January 2017 – “Minimum requirements for the risk management of asset management companies” (Mindestanforderungen an das Risikomanagement von Kapitalverwaltungsgesellschaften, “**KAMaRisk**”) as well as the BaFin Cloud Guidance;

**Insurance companies:** The key framework for outsourcing by credit institutions is set out in section 32 of the German Insurance Supervisory Act (Versicherungsaufsichtsgesetz), Art. 274 of the Commission Delegated Regulation (EU) 2015/35, the Minimum Requirements for the Governance System of Insurance Companies (Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGO)), the Minimum Requirements for the Governance System of Small Insurance Companies (Aufsichtsrechtliche Mindestanforderungen an die Geschäftsorganisation von kleinen Versicherungsunternehmen nach § 211 VAG (MaGo für kleine VU)), the Supervisory Requirements for IT in Insurance Companies (“Versicherungsaufsichtsrechtliche Anforderungen an die IT”) as well as the BaFin Cloud Guidance; and

**Payment services providers:** The requirements on outsourcing specifically for payment services providers are set out in section 26 of the German Payment Services Supervisory Act (Zahlungsdiensteaufsichtsgesetz) as well as the BaFin Cloud Guidance. While the outsourcing rules of the MaRisk do not explicitly apply to payment services providers, BaFin has indicated that they serve as indications for the requirements of a proper business organisation in this regard.

Whilst they are subject to deviations in detail, the outsourcing rules applicable to financial institutions (i.e., credit institutions and investment firms), fund managers, insurance companies and payment services providers broadly address the same requirements. The following overview relates to the outsourcing rules applicable to financial institutions.

## General regulatory framework for outsourcing of processes and activities by financial institutions

The general regulatory framework for the outsourcing of processes and activities by financial institutions, as provided for in section 25b of the KWG and chapter AT 9 of the MaRisk, can be summarised as follows.

### Scope of application and the definition of outsourcing

Broadly speaking, in line with the European rules, the German outsourcing rules distinguish between material outsourcing (which corresponds to “critical” outsourcing under European rules; accordingly, in the following the term “critical” is used), other outsourcing, and the external procurement of services. This distinction is important for the determination of the regulatory rules to be observed. German law provides for detailed rules applicable to critical outsourcing. On the other hand, other outsourcing or procurement of services which does not qualify as critical must only comply with the general requirements on proper business organisation and, in case of IT services, the requirements set out in the BAIT (see below).

Critical outsourcing can be characterised as follows:

**Outsourcing.** “Outsourcing” is not defined in national German law. However, chapter AT 9 of the MaRisk indicates that BaFin considers that an outsourcing is the assignment by a financial institution, to another undertaking, of the performance of certain activities or processes related to the execution of banking transactions, financial services or other typical services that would otherwise be performed by the financial institution itself. If an assignment does not qualify as outsourcing, it is referred to as “other external procurement of services”. This is in line with the (directly applicable) definition of outsourcing in Article 2(3) of the MiFID II Delegated Regulation.

**Critical outsourcing.** A “critical outsourcing” is defined as per Article 30(1) of the MiFID Delegated Regulation as being: “where a defect or failure in its performance would materially impair the continuing compliance of an investment firm with the conditions and obligations of its authorization or its other obligations under MiFID II, or its financial performance, or the soundness or the continuity of its investment services and activities”. From a German perspective, this definition should be read in conjunction with chapter AT 9 sections 1 and 2 of the MaRisk which provides that the financial institution must conduct a risk analysis to determine whether an outsourcing relates to a critical activity or process.

Services which do not typically qualify as a critical outsourcing include the single or occasional procurement of goods or services from third parties, or services which are typically provided by regulated firms which, due to the factual circumstances or legal requirements, cannot be provided by the outsourcing institution itself at the time of such procurement or in the future (for example taking custody of customer assets pursuant to the law on deposits of securities (Depotgesetz)). In addition, Article 30(2) of the MiFID II Delegated Regulation sets out certain specific functions which are not to be considered as critical for the purposes of Article 30(1): the provision to the firm of advisory services and other services which do not form part of the investment business of the firm, including the provision of legal advice to the firm, the training of personnel of the firm, billing services and the security of the



firm's premises and personnel as well as the purchase of standardised services, including market information services and the provision of price feeds.

**Other external procurement of services.** The MaRisk also clarifies that, as a general rule, the isolated procurement of software is to be categorised as "other external procurement of services" and this includes the customisation of software to the requirements of the institution, programming, testing and implementation, maintenance and other support services. This does not apply in the case of software that is used to identify, assess, monitor, control and communicate risks or which is essential for carrying out banking tasks; in this case, support services have to be qualified as an outsourcing. Further, the operation of such software by an external third party qualifies as an outsourcing. As a next step, it has to be determined based on a risk assessment whether such outsourcing is to be qualified as a critical outsourcing.

### Requirements applicable to critical outsourcings

The key requirements with which a financial institution must comply when outsourcing critical operational functions are set out in Section 25b of the KWG which should be read in conjunction with chapter AT 9 of the MaRisk and Article 31 of the MiFID II Delegated Regulation (to the extent the outsourcing relates to functions which form part of the investment business). In Germany, the national rules and the directly applicable European rules partially overlap (i.e., there are occasions where the German rules apply in addition to Article 31 of the MiFID II Delegated Regulation):

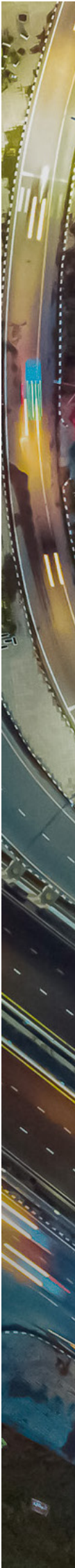
**Outsourcing agreements:** pursuant to sections 7 and 8 of chapter AT 9 of the MaRisk the following prescribed terms must be included in the outsourcing contract:

- specification and, if necessary, a description of the services to be performed by the outsourcing service provider (this requirement is not specifically set out in Article 31 of the MiFID II Delegated Regulation);
- safeguards for appropriate information and audit rights of the financial institution's internal audit function and its external auditors (this requirement is also addressed in Article 31(2)(i) of the MiFID II Delegated Regulation);
- unrestricted information and audit rights of the regulatory authority (this requirement is also addressed in Article 31(2)(i) of the MiFID II Delegated Regulation);
- rights to give instructions (this requirement is also addressed in Article 31(3) of the MiFID II Delegated Regulation);
- provisions to ensure that data protection and other security requirements are observed (this requirement is not specifically addressed in Article 31 of the MiFID II Delegated Regulation);
- appropriate termination rights (this requirement is also addressed in Article 31(2)(g) and Article 31(3) of the MiFID II Delegated Regulation);
- the obligation of the outsourcing service provider to notify the financial institution of any developments which could impair the orderly fulfilment of the outsourced activities and processes (this requirement is also addressed in Article 31(3) of the MiFID II Delegated Regulation); and
- specific contractual provisions relating to sub-outsourcing which:
  - guarantee that the firm continues to comply with the bank regulatory requirements (this requirement is not specifically addressed in Article 31 of the MiFID II Delegated Regulation);
  - provide for a consent requirement for sub-outsourcings by the outsourcing financial institution or, if such consent requirement is not possible, for concrete prerequisites for any sub-outsourcing or, at least, a requirement to ensure that the sub-outsourcing agreement is in line with the primary outsourcing agreement (this deviates from Article 31(3) of the MiFID II Delegated Regulation which requires that outsourcing by the service provider only takes place with the written consent of the investment firm); and
  - specify information and reporting obligations of the outsourcing service provider to the outsourcing financial institution (this requirement is not specifically addressed in Article 31 of the MiFID II Delegated Regulation).

Section 80(3) of the German Act on the Recovery and Resolution of Credit Institutions (Gesetz zur Sanierung und Abwicklung von Kreditinstituten), which transposes the European Recovery and Resolution Directive into German law, further requires that agreements on critical outsourcing must take into account the power of the resolution authority to require a financial institution under resolution, or any of its group entities, to provide any services or facilities that are necessary to enable a recipient to effectively operate the business transferred to it. We are not aware that this requirement is expressly provided for in the European rules.

**Risk management and monitoring requirements:** sections 9 and 10 of chapter AT 9 of the MaRisk require the outsourcing financial institution to control and monitor the risks associated with critical outsourcing, including periodic assessment of the performance of the outsourcing provider and the assignment of responsibilities for controlling and monitoring; section 6 requires appropriate business continuity planning/exit strategies for an expected or unexpected termination of the outsourcing agreement.





**Central outsourcing management:** pursuant to section 12 of chapter AT 9 of the MaRisk, the financial institution has to implement a central outsourcing management function (such central outsourcing management is not required under Article 31 MiFID II Delegated Regulation), to the extent required in light of the nature, scope and complexity of the outsourcing, which has to:

- produce and maintain complete documentation of all critical outsourcings;
- support all other internal departments regarding the legal and regulatory requirements related to outsourcing;
- co-ordinate and review the risk analysis underlying each outsourcing;
- implement and further develop an appropriate risk management framework including related control and monitoring processes; and
- provide an outsourcing report at least annually.

### Limitations regarding the scope of outsourced activities

BaFin has explicitly clarified in section 4 of chapter AT 9 of the MaRisk that, in general, activities and processes may be outsourced as long as this does not impair the orderliness of the business organisation pursuant to Section 25a KWG. However, certain limitations apply, in particular, under the following aspects (note that while the below appears more onerous than Article 31(1) of the MiFID II Delegated Regulation (please see page 6), the German regime generally reflects ESMA's opinions on outsourcing in the context of Brexit):

**No outsourcing of management board responsibilities:** the outsourcing must not lead to a delegation of management board responsibility to the outsourcing service provider (i.e., the management board cannot delegate the responsibility for the outsourced activities and processes to the outsourcing service provider). Further, management board functions cannot be outsourced. This includes, for example, the planning, co-ordination and controlling of the firm's business activities, the appointment of senior management functions, as well as the responsibilities specifically assigned to the management board under statutory rules (e.g., decisions on large exposures and determination of the business and risk strategies). Support functions below the level of the management board (e.g., risk control, compliance or internal audit), on the other hand, can be outsourced (subject to the further limitations described below).

**No impairment of supervision by BaFin:** any outsourcing must not prevent BaFin from performing its regulatory oversight (e.g., its right to request information, to audit and its ability to monitor). BaFin's ability to have oversight of an outsourcing financial institution must be ensured by means of suitable arrangements with regard to the outsourced activities and processes, including in the event of outsourcing to an enterprise domiciled in another EEA state or in a non-EEA state.

**Limitations regarding outsourcing of control functions:** complete outsourcing of the risk control function, the compliance function and the internal audit function is only permissible for subsidiary entities within a group if the outsourcing provider is the superordinate institution and the outsourcing subsidiary entity does not have to be considered significant: (i) by the national finance industry with regard to its size, complexity and the risk level of its business activities; and (ii) in relation to its importance within the group. However, due to proportionality, smaller financial institutions may fully outsource both their compliance function and their internal audit function if establishing these functions internally is not appropriate given the size of the institution as well as the nature, scale, complexity and risk of the institution's business activities. Outsourcing individual activities and processes of the control functions and the internal audit function, however, remains a possibility for all financial institutions. However, we note that BaFin has indicated in an expert article that the risk control function, the compliance function and the internal audit function must remain with the financial institutions as far as possible.

**Outsourcing to service providers in third countries:** an outsourcing to service providers in third countries is generally possible. Certain restrictions apply with regard to the outsourcing of functions related to portfolio management services (see Article 32(1) of the MiFID II Delegated Regulation and page 6 for more details).

### Summary of specific rules regarding certain areas of outsourcing by credit institutions and/or investment firms

With regard to certain areas of outsourcing, the German regulatory framework provides for specific requirements and restrictions, including in particular the outsourcing of: (i) control functions and core bank areas; (ii) the compliance function and compliance activities of investment firms; (iii) AML related activities and processes; and (iv) IT services.

**Outsourcing of control functions and core bank areas:** Sections 4 and 5, chapter AT 9 of the MaRisk set out specific additional rules regarding the outsourcing of "special control functions" and "core bank areas", including the following:

- Scope of permissible outsourcing: as set out above, the risk control function, the compliance function and the internal audit function may, generally, not be fully outsourced (with certain exceptions in the case of intra-group outsourcings);
- Retention of sufficient own skills and expertise: outsourcing financial institutions must retain sufficient skill and expertise to ensure effective supervision of the service provided by the outsourced service provider, and in the case of an outsourcing of a "special control function" (e.g., risk control, compliance and internal audit), a commissioner for each such function has to be appointed. (This is a similar requirement to Article 31(2)(e) of

the MiFID II Delegated Regulation; however, it creates additional requirements when outsourcing “special control functions” in Germany.)

- Measures to ensure continuity: measures to ensure the continuity and quality of the outsourced activities and functions must be implemented with a view to the planned or unexpected termination of the outsourcing agreement. The financial institution must ensure that proper functioning can be continued in the outsourced area in the event that the outsourcing arrangement ends or the group structure changes. (This is a similar requirement to Article 31(2)(l) of the MiFID II Delegated Regulation, however, it creates additional requirements when outsourcing “special control functions” in Germany.)

**Outsourcing of the compliance function or compliance activities:** Chapter BT 1.3.4 of the MaComp provides for certain requirements specifically relating to an outsourcing of the compliance functions or compliance activities of financial institutions (investment firms and credit institutions providing investment services). The following summarises the key requirements that apply in addition to the general requirements set out above:

- **Management board responsibility.** All applicable regulatory requirements have to be complied with, both in case of a partial or a full outsourcing. The management board is responsible for compliance with the requirements, in particular for ensuring that the compliance function is established in a clear and transparent manner taking into account the individual circumstances.
- **Compliance officer.** The compliance officer can be either an employee of the financial institution, an employee of the outsourcing service provider or a self-employed person/freelancer. The responsibility of the compliance officer for the performance of the entire compliance function of the financial institution cannot be divided between separate people. The compliance officer is entitled to demand that both the financial institution and the outsourcing service provider make available to them the resources that are reasonably necessary for the proper fulfilment of the duties and responsibilities of the compliance officer. The compliance officer acts independently and when acting in this capacity is not bound by instructions from the outsourcing service provider. The same applies to the employees of the compliance function of the financial institution and/or the outsourcing service provider who report to the compliance officer.
- **Compliance function.** The financial institution may combine its own employees, employees of the outsourcing service provider, employees of other undertakings and/or self-employed/freelance experts into an individual single compliance function under the responsibility and control of the compliance officer. The compliance function should only be fragmented by outsourcing/delegation to more than one outsourcing service provider and/or by the use of any additional third-party service providers if such division is necessary for functional and/or technical reasons.
- **Clear control and responsibilities.** Prior to the performance of the outsourced activities of the compliance function, the compliance officer and the outsourcing service provider must agree in a clear and transparent manner whether, how and in which forms of co-operation such performance shall be organised under the responsibility and control of the compliance officer, such as in an institution-specific policy or in a service level agreement. Even where only individual compliance activities are outsourced, it must be ensured that instructions given by the compliance officer are directly binding on the employees performing such activities at the outsourcing service provider.
- **Due diligence.** Before choosing an outsourcing service provider, the investment firm must perform due diligence to ensure that the relevant regulatory requirements are complied with in the case of the outsourcing. The financial institution is responsible for ensuring that the outsourcing service provider has the necessary organisation and professional competence, human resources, material resources and other resources and that the relevant employees have the necessary expertise and access to all information, including IT systems, required for performing the outsourced compliance function in an effective and preventative manner.
- **Integration.** The financial institution must ensure that the outsourced compliance function is permanent in the firm’s governance structure. The chosen service provider must ensure that the roles of the compliance officer and of the employees of the compliance function are adequately discharged on an ongoing basis, including on the site of the financial institution as appropriate.
- **Monitoring.** The financial institution must effectively monitor that the service provider performs its duties adequately, on the basis of appropriate substantive criteria to be determined on an individual firm basis. The senior management of the financial institution is responsible for supervising and monitoring the outsourced compliance function and/or compliance activities and must have the resources and expertise necessary for such purpose. The senior management may appoint a specific person employed by the firm for the ongoing monitoring and supervision on their behalf.

**Outsourcing of IT services:** Part 8 of BAIT provides for guidelines and requirements in relation to the outsourcing and other external procurement of IT services. The key provisions can be summarised as follows:

- The introductory section of the outsourcing chapter of BAIT repeats that the requirements pursuant to chapter AT 9 of MaRisk have to be observed in case of an outsourcing and that the general requirements relating to a proper business organisation apply in the case of other external procurement of IT services.
- BAIT also sets forth general requirements which apply to all procurement of IT services. BAIT states that, given the fundamental importance of IT to the institution, a risk assessment has to be performed prior to each instance of other external procurement of IT services, but the institution can flexibly define the nature and scope of such risk assessment in the light of its general risk management. Such procurement of IT services has to be managed in line with the strategies, taking account of the institution’s risk assessment, and a complete, structured contract overview has to be maintained for this purpose.

- The underlying agreements have to take appropriate account of the measures derived from the risk assessment relating to other external procurement of IT services, and where relevant, the possibility of an outage of an IT service provider has to be taken into account and a related exit or alternative strategy has to be developed and documented.
- The risk assessments relating to other external procurement of IT services has to be reviewed and amended regularly and on an ad hoc basis, together with the contractual details, where appropriate.
- Section 9 of BAIT addresses financial institutions that are operators of so-called critical infrastructures pursuant to the Act on the Federal Office for Information Security (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, “BSI Act”) in connection with the corresponding BSI Kritis Regulation (BSI-Kritisverordnung). It sets out additional guidance on how to comply with the requirements of the BSI Act and emphasises that these requirements also need to be considered in the case of outsourcings. Compliance with section 9 is optional, but serves as a basis for evidencing compliance with the BSI Act (as required by section 8a(3) of the BSI Act at least every two years).
- In addition to BAIT, the BaFin Cloud Guidance provides further guidance for an outsourcing to cloud services providers.

**Outsourcing of AML processes and activities:** the GwG, which transposes MLD/MLD5 into German law, contains certain provisions regarding the performance of AML related activities by third parties. The rules differentiate between: (i) the performance of client due diligence obligations by certain qualified third parties (Section 17(1) GwG); and (ii) the outsourcing of the client due diligence obligations to other third parties (section 17(5) GwG):

- Performance of customer diligence obligations by certain qualified third parties: pursuant to section 17(1) of the GwG, a firm may rely on a third party for the purpose of fulfilling client due diligence obligations, including, amongst others, on other undertakings obliged to comply with the anti-money laundering obligations under the GwG or the MLD or undertakings resident in a third country, provided these are subject to equivalent due diligence and record retention requirements and equivalent supervision (except if the undertaking is resident in a country with high money laundering risks). The firm does not have to comply with the general outsourcing rules in this case. The obliged entity has only to ensure that the third party:
  - identifies persons domiciled in Germany in accordance with the requirements of the GwG;
  - collects the information that is necessary for fulfilment of the client due diligence obligations;
  - promptly and directly forwards this information to the financial institution; and
  - promptly presents to the financial institution, upon request, copies of those documents that are relevant for identification and verification of the identity of the client, persons acting on behalf of the client and the ultimate beneficial owner(s), as well as all other relevant documents.
- Outsourcing to other third parties: any outsourcing of customer due diligence obligations to other third parties must comply with the general outsourcing rules and the specific rules set out in section 17(5) of the GwG. The latter requires, amongst others, the following:
  - The commissioned person or undertaking has to be suitable for the fulfilment of the due diligence obligations and has to comply with the requirements of the GwG;
  - The obliged entity has to ensure that the third party fulfils the same requirements set out above for the case of qualified third parties;
  - The transfer may not impair:
    - the fulfilment of the obligations by the obliged entity;
    - the ability of the senior management of the obliged entity to manage and control; and
    - the supervision by the supervisory authority over the obliged entity;
  - Unless the commissioned person or undertaking is not a German embassy, foreign trade chamber or consulate:
    - the obliged entity has to ensure the reliability of the persons or undertakings to which he wants to transfer measures; and
    - during the term of the co-operation, the obliged entity has to ensure the appropriateness and orderliness of the measures taken by the commissioned persons or undertakings through spot checks;
  - There may not be an additional excessive risk through the transfer:
    - any outsourcing must not affect the proper conduct of businesses and services;
    - an adequate and effective risk management must be maintained by the commissioned persons or undertakings; and
    - the outsourcing must not result in a transfer of responsibility of the managing directors to the service providers.

## Benchmark Regulation

The requirements relating to the outsourcing of functions in the provision of a benchmark set forth in Article 10 of the BMR are directly applicable in Germany. BaFin has not issued any additional legislations or guidance regarding the same.

## GDPR

While GDPR applies directly in Germany, Germany has made use of opening clauses in the GDPR and passed a Federal Data Protection Act (Bundesdatenschutzgesetz, "**BDSG**"). The BDSG does not contain any provisions which are specifically related to outsourcing. However, it provides for some deviations from and exceptions to the rights of the data subject (Chapter III of the GDPR). Furthermore, it provides that certain violations against provisions of the BDSG related to consumer credit constitute administrative offences with fines of up to EUR 50,000. Some violations of the GDPR are qualified as criminal offences which can lead to imprisonment of up to three years.



# Ireland

## Central Bank of Ireland

The Central Bank of Ireland (the “**Central Bank**”) is both the prudential and financial conduct supervisor of Regulated Financial Service Providers (“**RFSPs**”) in Ireland.

The Central Bank’s mandate is to “*ensure financial stability, consumer protection and market integrity*”. Central to this is the use of risk-based supervision to challenge the effectiveness of the governance and risk management frameworks put in place by RFSPs. The rise in the utilisation by RFSPs of outsourcing service providers for the provision of services and/or activities, which are key to such RFSPs’ strategic objectives, along with a serious breach of outsourcing obligations by Ulster Bank in 2012 (discussed in more detail below) has resulted in the Central Bank increasing its focus on outsourcing in recent times.

## Outsourcing – The Irish Context

In November 2018, the Central Bank published a discussion paper on outsourcing activities in the financial services industry (DP8 – Outsourcing – Findings and Issues for Discussion (“**DP8**”). DP8 represents the most up to date communication/guidance on the Central Bank’s position on outsourcing. However, it should be emphasised that the content of the guidance is “*supplemental to existing sectorial regulations and guidance on outsourcing*”. Further the Central Bank goes on to state that “*it is a regulated firm’s responsibility to ensure that it is compliant with all of the relevant laws, regulations and guidelines.*”<sup>6</sup> Consequently, one could describe DP8 as sitting as an additional layer on top of existing laws, regulations and guidelines as detailed in Parts One and Two.

### Outsourcing Review Methodology Applied

The Central Bank carried out a ‘stocktake’ of previous supervisory engagements including themed inspections, full-risk assessments and targeted risks assessments which revealed deficiencies in the governance and risk management practices applied to some outsourcing arrangements. On this basis, the Central Bank deemed it necessary to perform an in depth review of this area. This was achieved through a “*Cross Sector Survey of Regulated Firms on Outsourced Activities*” (the “**Survey**”) which was issued to a representative group of regulated firms across the financial services industry (insurance firms, banks, payment institutions, asset management firms). The Survey was completed by 185 regulated firms with high, medium-high or medium-low PRISM<sup>7</sup> impact ratings.

In DP8, the objective of the Survey was described as gathering cross-sectoral data in a number of areas including:

- the current pattern of outsourcing across RFSPs;
- whether outsourced activities are critical or important;
- how outsourcing risks are controlled;
- concentration risk;
- chain outsourcing;
- offshoring and any potential country risk; and
- sensitive data stored/processed by Outsource Service Providers (“**OSPs**”).

### Outcomes of the Survey

The Survey results were analysed to establish a cross-sectoral baseline view of outsourcing activities and related risks in RFSPs. The 185 RFSPs surveyed reported having a collective total of approximately 7,700 outsourcing arrangements in place and the Central Bank received data in respect of approximately 3,600 of those arrangements. DP8 presents the outcomes of the Survey in two parts. The first part relates to the findings of the Survey and the expectations of the Central Bank as a consequence, and the second relates to key risks and evolving trends which the Central Bank observed and on which they have sought feedback from RFSPs.

The Central Bank describes the key findings of the Survey as including “significant risk management deficiencies, on a widespread basis, in respect of a number of aspects of outsourcing risk management”. The Central Bank grouped these under the core functions of Governance, Risk Management and Business Continuity Management and discusses these in some detail. While the findings are important for RFSPs to understand, the expectations which the Central Bank details are of the greatest importance.

<sup>6</sup> The legislative requirements for RFSPs in Ireland, in the area of outsourcing, are largely derived from European legislation, as outlined in Part 1 of this document. However, the one exception is in relation to fund administrators. Chapter 2 of Part 4 of the Central Bank (Supervision and Enforcement) Act 2013 (Section 48(1)) (Investment Firms) Regulations 2017 [S.I. No. 604 of 2017] sets out the outsourcing rules for fund administrators in Ireland. This chapter addresses outsourcing in significant detail.

<sup>7</sup> The Central Bank’s risk-based supervisory framework – Probability Risk and Impact System.



## Minimum Supervisory Expectations

As mentioned above, in light of the key findings of the Survey, the Central Bank identifies in DP8 what it deems to be “the most obvious and minimum supervisory expectations around the management of outsourcing risks and focuses on the most basic areas of responsibility for the boards and senior management”. It does this under the core functions of Governance, Risk Management and Business Continuity Management and presents these expectations in user friendly lists for RFSPs, the details of which are set out in full below given the emphasis placed on them by the Central Bank:

### Governance

- Boards must have appropriate oversight and awareness of current and proposed outsourcing arrangements, evidenced by records of discussions and decisions in this regard;
- RFSPs must consider the extent and nature of their current and proposed outsourcing and any strategy devised must inform a comprehensive outsourcing policy which is approved by the board;
- RFSPs must have appropriate skills and knowledge to effectively oversee outsourcing arrangements, from inception to conclusion, particularly in the case of OSPs using emerging technologies;
- Operational oversight of outsourcing risk and outsourcing arrangements must be clearly designated to relevant individuals, functions and/or committees, to enable a holistic view of outsourcing to be maintained and reported on;
- RFSPs must have robust contracts and Service Level Agreements (“**SLAs**”) in place with their OSPs;
- The outsourcing of any Preapproved Control Function (“**PCF**”) or Control Function (“**CF**”) function must not affect the ability of senior management to make decisions and must never result in the delegation of senior management responsibilities;
- Outsourcing does not lower the suitability requirements applied to members of a RFSP’s management body, persons responsible for the management of the RFSP and its key functions holders;
- RFSPs must ensure that they are complying with their relevant obligations in relation to any existing or proposed outsourcing of a PCF or CF function;
- RFSPs which outsource the operational tasks of internal control functions for the monitoring and auditing of outsourcing arrangements, must ensure the operational tasks are effectively performed, including receiving appropriate reports, and exercise appropriate oversight and be able to manage the risks that are created by outsourcing arrangements;
- Third-party OSP and intra-group outsourcing arrangements are subject to the same governance and risk management principles; and
- Similarly, the same governance and risk management requirements are applied to ‘partnerships’ with Fintechs, Regtechs and Credit Service Providers, as are applied to traditional outsourcing arrangements to ensure all regulatory obligations are being met.

### Risk Management

- RFSPs’ risk management framework must appropriately consider any outsourcing arrangements;
- RFSPs must conduct comprehensive risk assessments in respect of any proposed outsourcing arrangement and these risk assessments must be tailored to take account of specific risks associated with outsourcing, including those set out in this Paper;
- RFSPs must consider and document the controls to be put in place to minimise exposure to any risks identified and these controls must be reflected in the relevant outsourcing contracts;
- RFSPs must have a ‘criticality and importance of service’ methodology that can be applied consistently across all outsourcing decisions and is in line with relevant sectoral regulations and guidance;
- The criticality or importance of outsourced service must be assessed on an ongoing basis;
- RFSPs must maintain sufficient skills and knowledge within the organisation to effectively oversee and challenge the performance of outsourcing arrangements and ensure that functions can be taken back in-house by the RFSP or substituted in an orderly manner, if required;
- RFSPs must monitor the performance of their OSPs and have mechanisms in place for the escalation and resolution of any issues identified;
- RFSPs must retain all responsibility for their strategy and policies where some or all of a risk management function is outsourced;
- RFSPs must ensure that their risk management structures are in line with relevant guidelines; and
- RFSPs must ensure that the governance and risk management structures they have in place around the outsourcing of IT systems and services are in line with the Central Bank’s Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks.

### Business Continuity Management (“**BCM**”)

- BCM is a consideration of RFSPs when proposing to engage the services of an OSP;
- RFSPs must ensure that where an outsourcing arrangement is in place, all governance surrounding such an arrangement, including business continuity plans and exit strategies are updated to reflect the variances in service delivery that such an outsourcing arrangement presents;

- RFSPs must have back up measures in place and consider, plan and test scenarios which may warrant the transfer of activities to another OSP or back in-house;
- Skills and expertise must be developed and maintained so that functions can be taken back in-house by the RFSP or substituted in an orderly manner, if required;
- RFSPs must have appropriate exit strategies in place where outsourcing arrangements are utilised and that these strategies allow for a timely and orderly transfer of activities with minimum service disruption;
- RFSPs must adhere to the relevant sectoral regulatory requirements and guidelines in relation to business continuity plans and exit strategies, when availing outsourcing arrangements;
- When testing their own business continuity plans, RFSPs must ensure that their OSPs are included in the testing of any activities or processes that involve or rely on a service provided by the OSP;
- RFSPs must ensure the OSP has a business continuity plan in place, which includes the outsourcing arrangements and that regulated firms ensure that they can participate in the OSP's business continuity plan testing; and
- RFSPs must regularly review the appropriateness of their business continuity plans and resilience measures in respect of outsourced activities, particularly in the context of new and evolving technologies, trends and risks.

### Key risks and evolving trends

In Part B of DP8, the Central Bank considers some of the key risks and evolving trends associated with outsourcing practices. For example, it notes the expansion in the scale and scope of outsourcing and in particular, the significant increase in outsourcing of risk management and internal control functions. It observed that a large proportion of outsourcing arrangements involve sensitive customer and business data and flagged the significance of concentration risk for some RFSPs, both in terms of concentration of OSPs used by the sector and the geographic locations where these OSPs are located. The Central Bank states that "all of these issues weaken the resilience of not only the regulated firms operating here, but of the wider financial sector in general given both the growing number of interdependencies and concentrations". In respect of these issues, the Central Bank details what it expects RFSPs to do in response and requests that they can "evidence" that this has been done, if called upon to do so. Finally, the Central Bank posed a number of questions on which it asked RFSPs to respond to the Central Bank.

### Central Bank conference on outsourcing

In April 2018, as a result of the responses received from RFSPs and interested bodies to the questions posed in DP8, the Central Bank held a conference on outsourcing to discuss the evolving risks associated with outsourcing and to determine whether further guidance or policy is required in this area.

There were various speeches from regulators worldwide as well as from Ireland along with three panel discussions. The panel discussions focused on the regulation of effective outsourcing relationships, emerging risks in complex outsourcing relationships and the use of the 'Cloud' and the management of sensitive data.

Gerry Cross, Director of Financial Regulation – Policy & Risk, at the Central Bank, closed the event summarising the key points considered during the conference. Mr Cross advised that the Central Bank "will reflect on the discussion points in its consideration of the appropriate regulatory response to evolving risks and trends in outsourcing going forward, and our consideration of the responses received in relation to the outsourcing discussion paper." There has been no further commentary or guidance from the Central Bank since this date. Consequently, until further communication is issued, what is detailed in DP8 is the Central Bank's current position on outsourcing by Irish RFSPs.

### Brexit

As part of Brexit contingency planning, a number of UK and US firms identified Ireland as a jurisdiction to establish a RFSP. As part of the authorisation process, the Central Bank focused in great detail on proposed outsourcing arrangements by such firms. The concern of the Central Bank was/is that once authorised, RFSPs would outsource all substance or the majority of their business to entities within their group, in order to circumvent regulation and supervision by the Central Bank. The Central Bank has therefore restricted some outsourcing arrangements as part of the authorisation. Subsequently, as part of their on-going supervision priorities, the Central Bank has continually reviewed such outsourcing arrangements and challenged senior management's oversight in this regard.

RFSPs are required to obtain the Central Bank's prior approval before introducing a material change to their business. Material change is intentionally not defined and the Central Bank adopts a broad interpretation of 'material change' and a broad interpretation as to what constitutes 'outsourcing'. On that basis, RFSPs should always assess whether any proposed arrangement with a third party or group entity amounts to an outsourcing arrangement that should be notified to the Central Bank and whether such arrangement would constitute a 'material change' to their business triggering the obligation to obtain prior approval from the Central Bank.

## Enforcement

The Central Bank's enforcement powers are derived from the Central Bank and Financial Services Authority of Ireland Act 2004 and were strengthened by the Central Bank (Supervision and Enforcement) Act 2013. The Central Bank employs two processes to ensure that RFSPs and individuals are held to account: the Administrative Sanctions Procedure ("**ASP**") and the Fitness and Probity Regime. For the purposes of this discussion on outsourcing, we will focus on the ASP.

Under the ASP, the sanctions for RFSPs include a caution or reprimand, suspension or revocation of authorisation, and/or a fine of up to €10 million or 10% of the RFSP's turnover. An individual, meanwhile, may be subject to disqualification from managing a RFSP for a specified period, and/or a fine of up to €1 million. The Central Bank has taken enforcement action regarding the failure by RFSPs to ensure that outsourced regulated activities are compliant with the relevant regulation. The following is a brief summary of a key action taken in the area of outsourcing.

### Ulster Bank

In 2014, the Central Bank fined Ulster Bank Ireland ("**Ulster Bank**") a then record €3.5 million for a failure to have robust governance arrangements in place in relation to its IT services which it outsourced to the Royal Bank of Scotland Group. The failings on the part of Ulster Bank resulted in an unprecedented situation where approximately 600,000 customers were deprived of essential and basic banking services over a 28 day period. This caused widespread and significant loss and inconvenience for customers.

In the settlement agreement, Director of Enforcement at the Central Bank, Derville Rowland stated that "while the Central Bank recognises that IT outsourcing is a feature of modern banking business, outsourcing is no defence for regulatory failings. Ultimate accountability for compliance remains with firms and they must ensure that they maintain oversight of outsourced activities. Senior management must ensure that risks associated with outsourced activities are appropriately managed and must be aware that outsourcing arrangements can never result in the delegation of their responsibility to manage the risks associated with such activities".

In 2016, Ulster Bank was again fined for outsourcing breaches. On this occasion it was fined €3.325 million for significant failings in the outsourcing, risk assessment and customer due diligence associated with its anti-money laundering/countering the financing of terrorism framework and procedures.

In the context of the outsourcing requirements, of which there were eight, including "two significant failings", Ulster Bank failed to put: (i) an outsourcing policy in place for an 11 month period; and (ii) an SLA in place for 19 of the 25 outsourced activities when the outsourcing commenced, as was required by its own outsourcing policy.

In the settlement agreement, Derville Rowland stated that the case "highlights that firms who outsource must have in place appropriate controls to oversee outsourced activity, which must be documented and clear. This is even more critical where the outsourcing is within the group because these situations tend to foster a misplaced sense of complacency regarding regulatory compliance".

# Italy

## Italian Consolidated Financial Act

The Italian Legislative Decree no. 58/1998 (Testo unico delle disposizioni in materia di intermediazione finanziaria, as amended, the “**Italian Consolidated Financial Act**”) is the main source of financial market law in Italy. The Italian Consolidated Financial Act also grants the power to issue secondary rules on certain technical aspects of financial regulation. Since its entry into force, the Italian Consolidated Financial Act has been amended several times in light of the multiple regulatory interventions from the European authorities on financial matters, including in connection with the MiFID II directive.

### Who does it apply to?

The Italian Consolidated Financial Act is composed of six sections and regulates an extremely wide range of financial institutions and activities relevant to the financial sector. The following provisions are of particular relevance to the outsourcing of financial services:

- Part II, which sets out a comprehensive set of rules on financial intermediaries, including: the supervisory powers entrusted to the Italian National Commission for Companies and the Stock Market (Commissione Nazionale per le Società e la Borsa, “**CONSOB**”) and the Bank of Italy; rules on the provision of investment services; rules relating to financial institutions providing investment services (such as investment banks); rules relating to how such services should be carried out (including in the case of outsourcing); and
- Part III, which sets out the rules on the management of the trading venues and centralised management of financial instruments (including outsourcings).

### Key definitions

- “**SGR**” means an asset management company;
- “**SICAV**” means an open-ended investment company;
- “**SICAF**” means a closed-ended investment company; and
- “**trading venue**” means a regulated market, a multilateral trading facility (MTF) or an organised trading facility (OTF).

### Outsourcing of services by SGRs, SICAVs and SICAFs

Pursuant to Article 33(4) of the Italian Consolidated Financial Act, SGRs, SICAVs and SICAFs may outsource specific functions related to the provision of financial services to external services suppliers provided that such financial institutions adopt proper procedures in order to avoid a drastic reduction of the services provided by the SGR, SICAV and SICAF through the external service provider.

In addition, an outsourcing must not affect the responsibility of the SGRs, SICAVs and SICAFs towards their investors in relation to the activities carried out through the outsourced services providers.

#### Outsourcing of services by trading venues

Pursuant to Article 65-sexies(6) of the Italian Consolidated Financial Act, CONSOB shall approve any agreement entered into by the manager of a trading venue for the outsourcing of critical operational functions relating to algorithmic trading.

For the purpose of Article 65-sexies(6) of the Italian Consolidated Financial Act, critical operational functions means one of the following:

- risk management procedures and systems to identify and manage the risks that may affect the activities of the trading venue and the measures to mitigate such risks;
- measures to ensure the sound management of the technical operations of the trading venue, including effective emergency measures to address the risks of system failures; or
- effective measures to simplify the settlement of the transactions executed within the system of the trading venue.

## Italian Consolidated Banking Act

The Italian Legislative Decree n. 385/1993 (Testo unico delle leggi in materia bancaria e creditizia, as subsequently amended, the “**Italian Consolidated Banking Act**”) is the main source of banking and credit law in Italy and the supervisory activities thereof. The Italian Consolidated Banking Act also grants the power to issue secondary rules on technical aspects of financial regulation, and to adopt prudential measures. Since its entry into force, the Italian Consolidated Banking Act has been amended several times in light of the multiple regulatory interventions from the European authorities on banking and credit-related matters.

### Who does it apply to?

The Italian Consolidated Banking Act regulates certain entities such as banks and other licensed entities, including payment institutions and electronic money institutions (for the purposes of this paragraph, the “**Licensed Entities**”), as well as the activities relevant to the banking and credit sector.

### Key definitions

- “**bank**” means the entity authorised to carry on banking activities.

### Supervision on outsourced services and activities

The Italian Consolidated Banking Act grants to the Bank of Italy certain supervisory powers and duties in relation to, inter alia: (i) specific information flows between the Bank of Italy and the Licensed Entities; (ii) certain powers of intervention on corporate bodies, on their members and on certain other corporate activities; and (iii) supervisory controls and assessments.

The above provisions also apply to any subject and entities to whom the Licensed Entities have outsourced essential or important business functions.

## Bank of Italy Circular No. 285 Of December 17, 2013 – Prudential Supervisory Instructions for Banks

On December 17, 2013 the Bank of Italy adopted the Circular no. 285 on prudential supervisory instructions for banks (“**Circular 285**”). Circular 285 is made up of four parts, characterised by different layouts reflecting the different scope and nature of the regulatory powers that can be exercised by the Bank of Italy. Parts one and two deal with the provisions transposing and implementing CRD IV and Regulation (EU) 575/2013 (Capital Requirements Regulation) (the “**CRR**”) respectively. Part Three contains prudential provisions on matters and types of risks not covered by either the CRD IV or the CRR, while part four contains provisions relating to particular intermediaries.

Circular 285 also takes into account the international standards of the Basel Committee (especially Basel 3) as well as the EBA Guidelines.

### Who does it apply to?

Circular 285 applies to Italian banks and banking groups. Certain provisions apply also to Italian branches of EU and non-EU banks.

### Timing

Circular 285 was first adopted on December 17, 2013 and has been amended and supplemented several times through the years to reflect regulatory changes at both European and national level (the latest amendment was dated December 2019).

### Scope

Circular 285 provides for the prudential supervisory provisions applicable to Italian banks and banking groups, revised and updated in order to adapt the internal regulations to the new international regulatory framework with particular regard to the new regulatory and institutional framework of banking supervision in the European Union.

Circular 285 distinguishes between provisions covering: (i) outsourcing of functions outside the banking group; and (ii) outsourcing of functions within the banking group.

### Key definitions

- “**body charged with strategic supervision**” means the corporate body charged with the functions of direction and/or supervision of the company’s management (for example, by examining and resolving on the company’s industrial or financial plans or strategic operations);
- “**management body**” means the corporate body or the members of the corporate body to which management tasks are assigned or delegated (for example, the implementation of the guidelines adopted in the exercise of the strategic supervision function);
- “**corporate control functions**” means the compliance function, the risk management function, and the internal audit function;
- “**control functions**” means all the functions which, by virtue of a legislative, regulatory, statutory or self-regulatory provisions, are entrusted with control responsibilities;



- **“important operational function”** means an operational function for which at least one of the following conditions is present:
  - an anomaly or failure in its execution can seriously jeopardise: (a) the financial performance, soundness or continuity of the bank’s business; or (b) the bank’s ability to comply with the conditions and obligations arising from its authorisation or obligations under supervisory regulations;
  - concerns activities reserved as important by law; or
  - concerns operational processes of the company’s control functions or has a significant impact on the management of corporate risks, and
- **“outsourcing”** means an agreement in any form between a bank and a service provider whereby the provider implements a process, service or activity of the same bank.

### Outsourcing of functions outside the banking group

Banks resorting to outsourcing shall monitor the risks arising from the choices made and maintain the control capacity and responsibility for the outsourced activities, as well as monitoring the technical and managerial skills essential to re-internalise, if necessary, their performance.

The decision to outsource the performance of certain functions (even not important ones) shall be consistent with the company’s outsourcing policy. The outsourcing policy is adopted by the body charged with strategic supervision and implemented by the management body. In line with the principle of proportionality, the outsourcing policy provides for at least:

- the decision-making process for outsourcing business functions;
- the minimum content of outsourcing contracts and the expected service levels of outsourced activities;
- the ways in which the outsourced functions are monitored, continuously and with the involvement of the internal audit function;
- internal information flows aimed at ensuring that corporate bodies and control functions have full knowledge and control over the risk factors relating to outsourced functions; and
- business continuity plans (contractual clauses, operational plans, etc.) in the event of improper performance of the outsourced functions by the service provider.

In any case, through outsourcing, banks shall not:

- delegate their responsibilities, or the responsibility of their corporate bodies;
- alter the relationship and obligations towards their clients;
- jeopardise the ability to comply with their obligations under the supervisory regulations or to breach the reserves of activity provided for by law;
- undermine the quality of the internal control system; or
- obstruct supervision by the supervisory authorities.

### Outsourcing of important operational functions

Without prejudice to the requirement to ensure proper performance by the outsourced services supplier, proper functioning of the system of internal controls, and the continuous monitoring of the activity carried out by the service provider, if banks intend to outsource important operational functions they shall ensure that the following conditions are met:

- the written agreements between banks and service providers shall clearly provide the following information:
  - the respective rights and obligations of the parties;
  - the expected service levels, expressed in objective and measurable terms, as well as the information necessary to verify compliance with them;
  - any conflicts of interest and the appropriate precautions to prevent or, if not possible, mitigate them;
  - the conditions under which the agreement may be amended;
  - the duration of the agreement and the arrangements for its renewal, as well as the reciprocal undertakings connected with the termination of the relationship; and
  - the levels of service provided in case of emergencies and the continuity solutions compatible with the company’s needs, consistent with the requirements of the supervisory authority. The outsourcing agreements shall also establish proper procedures for participation by the bank, either directly or through user committees, in the verification of suppliers’ business continuity plans.
  - Moreover, the outsourcing agreements shall also provide termination clauses allowing the bank to terminate the outsourcing agreement in case of events which could compromise the supplier’s ability to guarantee the service or when the agreed service level is not met.
- the service provider shall:
  - have the competence, capacity and authorisations required by law to carry out the outsourced functions in a professional and reliable manner;
  - inform the bank of any event that might affect its ability to carry out the outsourced functions effectively and in compliance with the regulations in force; in particular, it shall promptly notify the occurrence of

- security incidents, also in order to promptly activate the relevant management or emergency procedures; and
- ensure information security in relation to the bank's activities, in terms of availability, integrity and confidentiality; in this respect, the service provider shall ensure compliance with the rules on personal data protection.
- the bank shall:
  - retain the power to effectively control the outsourced functions and to manage the risks associated with outsourcing, including those arising from potential conflicts of interest of the service provider;
  - identify within its organisation, a person with adequate professional skill and experience who will be responsible for the control of the outsourced functions (referente per le attività esternalizzate, the "Contact Person"); and
  - acquire the service provider's business continuity plans or have adequate information, in order to assess the quality of the planned measures and to integrate them with the continuity solutions implemented internally.
- the bank, its external auditors and the supervisory authorities shall have effective access to data relating to outsourced activities and the premises where the service provider operates. The right of access for the supervisory authority must be expressly stated in the contract, without additional burdens for the intermediary; and
- the contract with the service provider provides that any subcontracting relationships are agreed in advance with the bank and are defined in such a way as to allow full compliance with all the conditions listed above relating to the primary contract, including the possibility for the supervisory authority to have access to data relating to the outsourced activities and the premises in which the subcontractor operates.

### Outsourcing of corporate control functions (funzioni aziendali di controllo)

The outsourcing of corporate control functions to third parties with adequate professionalism and independence is usually allowed only for banks classified, for SREP purposes, in macro-category 4 (i.e., small institutions which do not fall under categories 1 to 3).

Banks that intend to outsource all or part of the corporate control functions shall provide in the outsourcing agreement:

- objectives, methodology and frequency of controls;
- methods and frequency of reporting due to the Contact Person for the outsourced activity and to the company bodies on the controls carried out (without prejudice to the fact that the Contact Person and the company bodies remain responsible for the correct performance of the outsourced control activities);
- confidentiality obligations on the information acquired in the performance of the function;
- connections with the activities carried out by the body with control function;
- the right to request specific control activities in case of sudden needs; and
- exclusive ownership by the bank of the results of the controls.

Banks shall appoint specific Contact Persons for each of the outsourced corporate control functions. A single Contact Person may be appointed for the outsourced second-level corporate control functions.

The service provider to whom the company's corporate control functions are to be outsourced must:

- be independent from the bank;
- not cumulate positions relating to second and third level corporate control functions<sup>8</sup> for the same bank or banking group;
- not simultaneously perform, for the same bank or banking group, tasks relating to corporate control functions and activities that it would be called upon to control as a service provider; and
- not perform external audit functions for the outsourcing bank or for other companies in the group to which it belongs.

In compliance with the same above conditions and according to the principle of proportionality, banks may also outsource specific controls, which require specialised professional knowledge, in operational areas of limited size and/or risk.

### Notifications to the European Central Bank or the Bank of Italy

Banks intending to outsource, in whole or in part, the performance of important operational or control functions shall notify the European Central Bank or the Bank of Italy in advance. The communication shall be made at least 60 days before appointing the service provider and shall specify the business needs that determined the choice. The European Central Bank or the Bank of Italy may start a procedure to prohibit the outsourcing within 60 days of receipt of the notification.

<sup>8</sup> Pursuant to Circular 285 Italian banks shall implement an adequate system of internal controls, which consist of controls of the business processes performed by the institution's business units themselves (first level controls), of the monitoring by the compliance function (second level controls) and of inspections by an internal auditing function (third level controls).

Before April 30 of each year, banks shall send to the European Central Bank or the Bank of Italy a report, drawn up by the internal audit function – or, if outsourced, by the company's Contact Person – with an evaluation of the body charged with control functions and approved by the body charged with strategic supervision, concerning the controls carried out on the outsourced important or control functions, outlining any deficiencies found and the relevant corrective action taken.

### **Outsourcing of cash management**

Given its inherent risks, Circular 285 sets out specific provisions for the outsourcing of cash management. In particular, without prejudice to the provisions concerning the outsourcing of important operational or control functions, banks outsourcing cash management activities shall adopt specific measures when choosing contractors and ensure the subsequent exercise of effective controls, which should be carried out continuously in order to verify the orderly and correct performance of the activity.

### **Outsourcing of functions within the banking group**

It is the parent company's responsibility to define the company's outsourcing policy within the banking group, and it must identify at least:

- the decision-making process for outsourcing business functions to the parent company or other members of the group;
- the measures taken to ensure adequate protection of the interests of any minority shareholders;
- the criteria for identifying the service provider within the group, and its obligations; in particular, with regard to important functions, the service provider shall:
  - have the knowledge, capabilities and authorisations required by law to carry out the outsourced functions in a professional and reliable manner;
  - inform the parent company and the outsourcing bank of any event that might affect its ability to carry out the outsourced functions effectively and in compliance with current regulations;
  - promptly notify concerned parties about the occurrence of safety incidents, in order to allow for the prompt activation of the relevant management or emergency procedures; and
  - ensure the security of information relating to the activities of the outsourcing bank in terms of availability, integrity and confidentiality, and ensure compliance with the rules on personal data protection;
- the minimum content of outsourcing agreements and the expected service levels of outsourced activities;
- the levels of service guaranteed in case of emergency and the contingency plans (which must be compatible with the company's needs and consistent with the supervisory authority's requirements); and
- information flows aimed at ensuring that the parent company, the broader group, outsourcing bank (including their corporate control functions) have full knowledge and governance of the risk factors relating to the outsourced functions.

A bank belonging to a banking group, without prejudice to its responsibility for outsourced activities, may waive the above outsourcing provisions (see "Outsourcing outside the banking group") provided that it complies with the outsourcing policy within the group. However, a bank must never:

- delegate its responsibilities, or the responsibility of corporate bodies;
- alter the relationship and obligations to his clients;
- jeopardise its ability to comply with its obligations under the supervisory regulations or to breach the reserves of activity provided for by law;
- undermine the quality of the internal control system; or
- obstruct supervision.

Notwithstanding the above, the parent company of a banking group (which is the entity with the power of direction and coordination of the affiliated banks and is responsible for the stability and sound and prudent management of the group) shall not outsource or delegate to any other entities the activities which fall under its exclusive responsibility.

### **Outsourcing of corporate control functions within the banking group**

Outsourcing of corporate control functions to the parent company or other members of the group is permitted, regardless of the size and operational complexity of the bank, in accordance with the following criteria:

- the costs, benefits and risks underlying the solution adopted are assessed and documented at group level with such assessment being periodically updated;
- the members of the group are aware of the choices made by the parent company and are responsible, each according to its own competences, for the implementation of the strategies and policies pursued in the field of controls, favouring their integration within the group controls; and
- within the banks of the group and the other entities which, in the opinion of the parent company, assume risks considered significant for the group as a whole, special Contact Persons are appointed who: (i) perform support tasks for the outsourced control function; (ii) report functionally to the outsourced control function; and (iii) promptly report particular events or situations, which are likely to change the risks generated by the subsidiary. A single Contact Person may be appointed for outsourced second-level control functions only.

## Outsourcing of ICT resources and services

In addition to the above mentioned rules on outsourcing within and outside the banking group, Circular 285 also provides for specific rules on outsourcing of ICT resources and services. In general, the outsourcing of ICT resources and services can take different forms depending on the architectural model adopted: from vertical outsourcing (related to certain operational processes) to horizontal outsourcing of transversal services such as hardware management (facility management), development and management of the application inventory (application management), network connections, technical help desk and repair and maintenance of ICT resources, up to full outsourcing of the overall corporate information system.

## Bank Of Italy Supervisory Provisions For Payment And Electronic Money Institutions

On July 23, 2019 the Bank of Italy adopted a new regulation amending the Supervisory Provisions for Payment and Electronic Money Institutions of May 17, 2016 in order to implement Directive 2015/2366/EU (“**PSD2**”) and its implementing provisions to coordinate the new provisions with the existing legislation (the “**Bank of Italy PI/EMI Regulation**”).

### Who does it apply to?

The Bank of Italy PI/EMI Regulation applies to:

- entities, natural or legal entities, intending to set up a payment institution (“**PIs**”) or an electronic money institution (“**EMIs**”) in Italy;
- existing companies wishing to be authorised in Italy as PIs or EMIs; and
- PIs wishing to amend the content of the authorisation.

### Timing

The Bank of Italy PI/EMI Regulation came into force on August 19, 2019.

### Scope

The Bank of Italy PI/EMI Regulation amended the rules already applicable to PIs and EMIs (as specified above) in order to ensure the common implementation of the PSD2, in relation to, inter alia, requirements for the application for authorisation and the procedure for its granting, requirements of equity holders and company representatives, activities to be carried out and the consequent prudential regulations, the administrative, accounting and internal control organisation, the rules applicable to branches, agents, contractual parties and the disposition for the regime of freedom to provide services, as well as information and inspection supervision activities.

### Key definitions

- “**company representatives**” means the persons who carry out administration, management and control functions, regardless of the name of the office;
- “**electronic money institutions**” means – as defined under Article 1(2)(h-bis) of the Italian Consolidated Banking Act – entities, other than banks, which issue electronic money;
- “**payment institutions**” means – as defined under Article 1(2)(h-sexies) of the Italian Consolidated Banking Act – entities, other than banks and electronic money institutions, authorised to provide payment services; and
- “**institution**” or “**institutions**” means an electronic money institution and an Italian payment institution.

### Internal governance

Institutions must adopt an outsourcing policy based on the EBA Guidelines.


Institutions shall periodically notify the Bank of Italy (in a report on the organisational structure drawn up in accordance with the format set out under Chapter IV, Annex D of the Bank of Italy PI/EMI Regulation, to be sent to the Bank of Italy by April 30 of each year), with reference to operational functions related to payment services, the issuance of electronic money or other important functions that the institution has outsourced as well as the procedures adopted for the control of these functions: (i) the outsourced functions and the contact person responsible for outsourced activities; and (ii) the content of the outsourcing agreements, including the identity and geographic location of the supplier and the procedures adopted for the control of outsourced functions.

### Outsourcing of critical or important functions

Pursuant to Chapter IV, Section II and Chapter IV, Annex B of the Bank of Italy PI/EMI Regulation:

- outsourcing of operational functions relating to payment services and the issuance of electronic money, as well as the system of internal controls or the outsourcing of the information system or critical components thereof, shall be notified at least 60 days in advance to the Bank of Italy. Subsequently, the Bank of Italy may start, within the following 60 days, a procedure to prohibit such outsourcing;
- the institutions wishing to outsource operational functions relating to payment services or the issuance of electronic money to a service provider established in an EU Member State shall inform the Bank of Italy at least 30 days in advance. The Bank of Italy shall notify, within the term of 30 days, the competent authority of





the host Member State of the information received and shall notify the institution involved of the notification to the competent authority of the host Member State;

- the electronic money institution wishing to use third party entities to distribute and redeem electronic money shall send a general outline of the agreement before proceeding to the Bank of Italy, which may start, within the term of 60 days, a procedure to prohibit such outsourcing (which is completed within 60 days). The individual agreements drawn up according to the scheme are not subject to specific notification to the Bank of Italy. However, the electronic money institutions shall record the relevant documentation and keep up-to-date information at the disposal of the Bank of Italy in relation to all the third party entities they make use of;
- institutions shall notify the Bank of Italy without delay of any significant changes in the information regarding outsourcing arrangements previously communicated;
- the outsourcing of important operational functions cannot materially jeopardise the quality of the internal control or prevent the Bank of Italy from monitoring the compliance with the applicable provisions;
- the outsourcing entity shall in any case ensure that: (i) outsourcing does not result in the devolution of responsibility from the corporate bodies; (ii) the relationship and obligations of the institution towards its customers is not affected; and (iii) compliance with the conditions which the institution must meet in order to be authorised to provide payment services or to issue electronic money and to maintain such authorisation; and
- entities entering into or implementing agreements to outsource operational functions related to payment services, or important functions, or to outsource the information system or critical components thereof, shall ensure that certain conditions relating, inter alia, to the competence, capacity and adequacy of the provider are met.



## Bank Of Italy Regulation Implementing Articles 4-Undecies and 6, Paragraph 1, Letter B) and C-Bis) of the Italian Consolidated Financial Act

On December 5, 2019 the Bank of Italy adopted a new regulation (the “**Bank of Italy Regulation as of December 5, 2019**” or the “**Regulation**”) in order to align the Italian rules governing certain matters falling within the exclusive jurisdiction of the Bank of Italy and relating to financial intermediaries providing investment services (such as investment banks) and asset management services, to the MiFID II and MiFIR provisions.

The Regulation has been adopted together with the entry into force of certain amendments to the Bank of Italy Circular no. 285 as of December 17, 2013 (the “**Italian Prudential Supervisory Instructions For Banks**”) adopted to implement the MiFID II and MiFIR provisions applicable to Italian banks.

### Who does it apply to?

The Bank of Italy Regulation as of December 5, 2019 applies to all Italian financial institutions which are:

- stock brokerage companies (“**SIM**”); and
- other financial intermediaries – such as banks, stockbrokers (agenti di cambio) and the so-called “Bancoposta” – when providing investment services and asset management services.

Certain provisions of the Regulation (specified below) apply only to financial institutions which are:

- SGR;
- SICAV; and
- SICAF,

which directly manage their assets.

### Timing

The Bank of Italy Regulation as of December 5, 2019 came into force on December 20, 2019.

However, pursuant to Article 2 of the Regulation, financial institutions which, as of the date of the entry into force of the Regulation, have ongoing agreements with cloud service providers, shall align the outsourcing agreements to the new rules on the date of the first renewal of the agreements and in any case not later than one year from the entry into force of the Regulation.

### Scope

The Bank of Italy Regulation as of December 5, 2019 modified the provisions applicable to certain Italian financial institutions (as specified above), in order to ensure the adoption by the same of organisational and operational systems to reduce operational risks and ensure sound and prudent management in relation to, inter alia, the outsourcing of critical or important operational functions. In particular, the purpose of the Regulation is to reorganise the Italian regulatory framework implementing the European standards set forth under the EBA Recommendations.

### Key definitions

- “**body charged with strategic supervision**” means the corporate body which – in accordance with the provisions of the Italian Civil Code and in accordance with the articles of association of the financial institution – is charged with the functions of direction and strategic supervision of corporate activities (such as the review and approval of the company’s strategic plan);
- “**cloud services**” means the services provided through cloud computing, a model that allows access on a convenient and on-demand network to a shared group of configurable IT resources (e.g., networks, servers, applications and services), which can be quickly provided and made available with a minimum of management activity or interaction with the service provider;
- “**EBA Recommendations**” means the recommendations on outsourcing to cloud services suppliers issued by the EBA on March 28, 2018 (EBA/REC/2017/03); and
- “**outsourcing**” means outsourcing as defined under Article 2(3) of Commission Delegated Regulation (EU) 2017/565: “an arrangement of any form between an investment firm and a service provider by which that service provider performs a process, a service or an activity which would otherwise be undertaken by the investment firm itself”.

### Internal governance

Institutions must adopt an outsourcing policy based on the EBA Recommendations.

The body charged with strategic supervision shall define, approve and periodically assess, the implementation of the outsourcing policy and the consistency of such policy with the activities of the financial institution.

## Outsourcing of critical or important functions

Pursuant to Article 18 of the Bank of Italy Regulation as of December 5, 2019:

- financial institutions shall adopt appropriate measures to mitigate the risks involved with the outsourcing of critical or important functions when entrusting an external service supplier with the performance of such services;
- the outsourcing of critical or important functions shall not reduce the effectiveness of the audits and inspections to which the financial institutions are subject nor prevent the Bank of Italy and CONSOB from assessing the fulfilment of their obligations by the financial institutions;
- the outsourcing of critical or important functions shall be managed in accordance with the provisions of Articles 30, 31 and 32 of MiFID II Delegated Regulation (set out above); and
- when outsourcing functions to external cloud services suppliers, financial institutions shall ensure compliance with Recommendation 4.2 of the EBA Recommendations, pursuant to which the outsourcing institutions should “make available to the competent authorities the following information:
  - the name of the cloud service provider and the name of its parent company (if any);
  - a description of the activities and data to be outsourced;
  - the country or countries where the service is to be performed (including the location of data);
  - the service commencement date;
  - the last contract renewal date (where applicable);
  - the applicable law governing the contract; and
  - the service expiry date or next contract renewal date (where applicable).”

Financial institutions shall transmit the information listed above to the Bank of Italy at least 30 days before outsourcing the functions to the external suppliers.

## Special provisions applicable to SGR, SICAV and SICAF

SGR, SICAV and SICAF managing assets whose value is above a certain threshold provided by Article 35-undecies of the Italian Consolidated Financial Act which plan to outsource critical or important functions, shall inform the Bank of Italy in advance, providing the following information:

- the functions which are to be outsourced, specifying whether the external service provider belongs to the same group of the financial institution;
- the purpose and the objective reasons behind the choice to outsource the functions;
- the criteria used to select the outsourcer;
- the resources deployed by the outsourcer to carry out its activity and the resources deployed by the SGR, SICAV and SICAF to oversee the services outsourced;
- the control mechanisms used to ensure the quality of the service (including the option to contact other suppliers in a timely manner and without prejudice to the functionality of the services outsourced) and the due observance of the confidentiality and regulatory constraints that may exist;
- the safeguards adopted in order to comply with the conditions for outsourcing provided by the Regulation;
- show the safeguards (penalties, termination clauses, etc.) adopted in case of events that could affect the outsourcer’s ability to provide the service outsourced or ensure the agreed service levels; and
- when outsourcing cloud services, the notice addressed to the Bank of Italy shall also include the information provided under Recommendation 4.2 of the EBA Recommendations.

Within 30 days from the receipt of the information listed above, the Bank of Italy may start an ex-officio administrative proceeding ending within the next 60 days, in order to prohibit the execution of the outsourcing agreement.

## Italian Markets Regulation

With resolution no. 20249 of December 28, 2017, CONSOB adopted a new market regulation (“**Markets Regulation**”) in order to align the Italian rules on trading venues previously in place to the MiFID II and MiFIR provisions.

The Markets Regulation provides a redefinition of the organisational and operational requirements for trading venues, as well as of the transparency requirements in case of the outsourcing of operational functions (please see the discussion above).

### Key definitions

- “**operational functions**” means all direct activities related to the performance and surveillance of the trading systems supporting the following elements:
  - upstream connectivity, order submission capacity, throttling capacities and ability to balance customer order entrance through different gateways;
  - trading engine to match orders;
  - downstream connectivity, order and transaction edit and any other type of market data feed; and
  - infrastructure to monitor the performance of the elements referred to above; and

- “**critical operational functions**” means those functions necessary to comply with the obligations referred to in Article 47(1)(b), (c) and (e) of Directive 2014/65/EU.

### Outsourcing of important functions by trading venues

Pursuant to Article 10 of the Markets Regulation, the managers of the trading venues which outsource important functions (including operational functions and critical operational functions) are responsible for the outsourced functions, shall maintain the power to direct the functions outsourced and shall adopt proper organisational measures to ensure:

- the integration of the outsourced services with the internal controls system of the trading venue;
- the identification of the risks connected to the outsourced services and the adoption of a detailed programme for their periodic monitoring;
- the adoption of proper control procedures on the outsourced services, including the establishment of a dedicated function and an appropriate data flow from the dedicated function to the administrative and control bodies; and
- the business continuity of outsourced services, acquiring information on the business continuity plans and disaster recovery measures adopted by the external services providers.

The managers of the trading venues shall define the purposes of the outsourced activities taking into account the global strategy of the company and maintain the process governance and oversee the related risks. To this purpose, trading venue participants shall have access to the information relating to the outsourced activities and evaluate the quality of the services rendered and the organisational and capital adequacy of the external services suppliers.

### Transparency requirements on outsourcing agreements

Pursuant to Article 38 of the Markets Regulation, trading venues shall promptly inform CONSOB of their intention to outsource operational functions (as defined above). To this purpose, the trading venues shall transmit to CONSOB a notice describing the outsourced activities, indicating, among other things:

- the measures adopted to ensure compliance with the provisions set forth under Article 10 of the Markets Regulation (described above) and Article 6 of the Delegated Regulation (EU) 2017/584;
- whether the external service provider is performing the same activities in the interest of other trading venues; and
- the timing of the outsourcing process.

If critical operational functions are outsourced, the trading venues shall also transmit to CONSOB, together with the information listed above, the full text of the outsourcing agreement.

The trading venues shall promptly notify to CONSOB the outsourcing of strategic activities, transmitting to the authority the outsourcing agreement.

If operational functions (as defined above) are outsourced, the trading venues shall also transmit to CONSOB a description of the services governed by the outsourcing agreement.

## Bank Of Italy AML Provisions

On March 26, 2019 the Bank of Italy adopted certain provisions on organisation, procedures and internal controls to prevent the use of financial intermediaries for money laundering and terrorism financing (the “**Bank of Italy AML Provision**”) in order to align the Italian legal framework with the applicable European provisions, and to implement certain amendments made by Legislative Decree 90/2017 to the Italian anti-money laundering law (Legislative Decree 231/2007, as subsequently amended, the “**Italian AML Decree**”) implementing the MLD.

### Who does it apply to?

The Bank of Italy AML Provision applies to:

- banks;
- SIM;
- SGR;
- SICAV;
- SICAF;
- authorised intermediaries registered in the register provided for under Article 106 of the Italian Consolidated Banking Act;
- electronic money institutions;
- payment institutions;
- branches established in Italy of banking and financial intermediaries having their registered office and headquarters in another EU country or in a third country state;
- banks, payment institutions and electronic money institutions having their registered office and headquarters in another EU Member State required to designate a central contact point in Italy in accordance with the Italian AML Decree;

- trust companies (società fiduciarie) registered in the register provided for under Article 106 of the Italian Consolidated Banking Act;
- trustees (confidi);
- micro-credit providers within the meaning of Article 111 of the Italian Consolidated Banking Act;
- Poste Italiane S.p.A., for the “bancoposta” activity; and
- Cassa Depositi e Prestiti S.p.A.,

(all the entities above, for the purposes of this paragraph, the “**Entities**”).

### Timing

The Bank of Italy AML Provision came into force on April 23, 2019.

The Entities shall comply with the provisions by June 1, 2019. However, the following provisions shall apply starting from January 1, 2020:

- the obligation for corporate bodies to define and approve a policy setting out the entity’s choices regarding organisational arrangements, procedures and internal controls, adequate assessment and data retention;
- the obligation for parent companies to establish a common reporting framework; and
- the obligation to carry out a self-assessment exercise on money laundering risks; the entities listed above shall transmit the results of the 2019 self-assessment exercise to the Bank of Italy before April 30, 2020.

### Scope

The Bank of Italy AML Provision introduced certain rules on organisation, procedures and internal controls to prevent the use of financial intermediaries for money laundering and terrorism financing purposes, in order to ensure, inter alia, the proper performance of anti-money laundering controls in cases of the outsourcings of certain services and/or activities so as not to jeopardise the quality of the system of controls.

### Key definitions

- “**AML Function**” means a dedicated internal function to prevent and counteract the implementation of money laundering transactions; and
- “**anti-money laundering risk**” means the risk arising from the violation of legal, regulatory and self-regulatory provisions aimed at preventing the use of the financial system for the purpose of money laundering, terrorism financing or financing of weapons of mass destruction development programmes, as well as the risk of involvement in money laundering and terrorism financing or the financing of weapons of mass destruction development programmes.

### Internal governance

Entities must establish a dedicated internal function to prevent and counteract money laundering (for the purpose of this paragraph, the “**AML Function**”), which shall assess, on an ongoing basis, that the Entity’s procedures are consistent with the objective of preventing and contrasting the violation of anti-money laundering regulations.

The performance of the controls attributed to the AML Function may be entrusted to external parties with appropriate requirements in terms of knowledge, authority and independence. The responsibility for the proper management of money laundering risks lies, in any case, with the Entities, which are required to assess such risks and maintain the technical and management skills required to assess the outsourced activities on a continuous basis.

In the event of outsourcing, the Entities appoint an internal manager to the anti-money laundering function (the “**AML Officer**”) with the task of verifying the proper performance of the service by the supplier and take the necessary organisational precautions to ensure that the powers of direction and control are maintained by the corporate bodies.

### Outsourcing of critical or important functions

The outsourcing agreements entered into by Entities with external suppliers shall, at least, set out the following information:

- their respective rights and obligations;
- the expected service levels, expressed in objective and measurable terms, as well as the information necessary to assess compliance with them;
- any conflicts of interest and appropriate measures to prevent or, if not possible, mitigate them;
- the duration of the agreement and the arrangements for its renewal, as well as mutual commitments related to the termination of the relationship;
- the minimum frequency of information flows to the internal manager and to corporate bodies and control functions, without prejudice to the obligation to promptly respond to any request for information and advice;
- the obligation of confidentiality relating to the information acquired in the performance of their duties;
- the possibility of revising the conditions of the service upon the occurrence of regulatory changes or in the operation and organisation of the Entities; and

- the possibility for the Entities, the applicable supervisory authorities and the UIF (Unità di Informazione Finanziaria) to access useful information and the facilities where the service provider operates for monitoring, supervision and control activities.

Notwithstanding the foregoing provisions on outsourcing within the groups, Entities with significant size and operational complexity are not allowed to outsource the tasks assigned to the AML Function due to the principle of proportionality.

For the outsourcing of the anti-money laundering function within the group (the so-called centralised model), the Entities shall apply the provisions on the outsourcing of control functions within the group laid down in the relevant sector-specific regulations to which they may be subject. In the absence of sector-specific rules, the AML Function may be outsourced to the parent company or other group company, regardless of the size and operational complexity of the Entity, in accordance with the provisions listed above.

Where groups do not use the centralised model and where the AML Function is outsourced only by certain group companies, the group companies that have not outsourced the function to the parent company or other group companies must:

- fully and promptly inform the AML Officer of the parent company or group of companies of the results of the control activities carried out at the company by the AML Officer, where relevant to the activity of the parent company or the group; and
- ensure that the AML Officer of the parent or group has access to all databases containing information relevant to the performance of the duties.



# Luxembourg

## Regulatory approach

Outsourcing plays a significant role in the Luxembourg financial market as many of the financial institutions are subsidiaries of foreign groups and therefore their operation is heavily reliant upon the outsourcing of services and activities. To illustrate this, a recent study<sup>9</sup> suggests that IT outsourcing is a €448 million market in Luxembourg, which represents 30% of the total information and communications technology services in Luxembourg.

The EBA Guidelines, as described in Part One, are considered the ultimate source of guidance on outsourcing activities by in-scope Luxembourg financial institutions. Soon after the EBA's publication of the EBA Guidelines, the Luxembourg Commission de Surveillance du Secteur Financier (the "CSSF") amended and aligned any guidance (i.e., CSSF Circulars) that was issued to that point on outsourcing rules with the EBA Guidelines. As discussed below, the EBA Guidelines are often more comprehensive than any corresponding CSSF guidance.

Luxembourg adheres to EU Regulations and swiftly transposes EU Directives into national law through various legislative tools with minimum or no "gold-plating". To this end, the Luxembourg legislative framework is harmonised with the EU-wide position stated in Parts One and Two.

## EBA and EIOPA Guidelines

As of 12 March 2020, the CSSF has published four Circulars (the "Outsourcing Circulars") which deal with outsourcing activities:

- CSSF Circular 12/552 on Central administration, internal governance and risk management, as amended by Circulars CSSF 13/563, CSSF 14/597, CSSF 16/642, CSSF 16/647 and CSSF 17/655;
- CSSF Circular 17/654 regarding IT outsourcing relying on a cloud computing infrastructure, as updated by Circular 19/714;
- CSSF Circular 17/656 on administrative and accounting organisation and IT outsourcing; and
- CSSF Circular 08/350 on the details relating to the amendments introduced by the Law of 13 July 2007 on markets in financial instruments, as amended by Circular CSSF 13/568.

The firms that are subject to the Outsourcing Circulars are also in-scope for the purposes of the EBA Guidelines (to which the laws of Luxembourg are closely aligned). Therefore, in-scope firms must read both the Outsourcing Circulars and the EBA Guidelines in conjunction with each other.

When comparing the EBA Guidelines with the Outsourcing Circulars the following observations can be made:

- the definition of 'outsourced activities' in the EBA Guidelines is much clearer than the Outsourcing Circulars as it provides an indication as to which functions do not consist of 'outsourced functions';
- The EBA Guidelines impose additional requirements on entities that outsource 'critical' functions, whereas, the Outsourcing Circulars merely oblige entities to obtain prior authorisation from the CSSF when contemplating outsourcings of a 'material function' (or notify the CSSF if the 'material function' is outsourced to a "support professional of the financial sector");
- The EBA Guidelines require authorisation for outsourcings of core or strategic functions, whereas, the Outsourcing Circular allows for such outsourcings subject to conditions;
- The EBA Guidelines require that an 'Outsourcing Policy' is implemented and is regularly reviewed and updated, whereas, the Outsourcing Circulars only require a business continuity plan for outsourcings of critical functions, and a pre-determined outsourcing approval process;
- The EBA Guidelines provide additional obligations and requirements to those found in the Outsourcing Circulars (e.g., the service provider must implement appropriate technical and organisational measures to protect personal or confidential data);
- The EBA Guidelines provide for a list of clauses that need to be included in outsourcing agreements, whereas the Outsourcing Circulars only requires an "official and detailed contract (including specifications)" without providing any further guidance on this.

As of the date of this Paper, the Commissariat aux Assurances, which supervises and regulates the insurance and re-insurance sector in Luxembourg, has not issued any specific guidelines on outsourcing for the entities which fall under its mandate nor has it yet endorsed the EIOPA Guidelines.

Finally, should any conflict arise between the Outsourcing Circulars and the EBA Guidelines, the Outsourcing Circulars should be followed.

---

<sup>9</sup> KPMG, 1 March 2019, "IT Outsourcing Provider Study", available at: <<https://home.kpmg/lu/en/home/insights/2019/02/it-outsourcing-provider-study-2018.html>>

## MiFID II and MiFID II Delegated Regulation

The Luxembourg Law of 30 May 2018 implemented MiFID II into Luxembourg law on 4 June 2018, whilst, the Grand-ducal Regulation of 30 May 2018 transposed the MiFID II Delegated Directive (EU) 2017/593 into Luxembourg law.

Article 16(5) of MiFID II on outsourcing for investment firms is reflected in Article 36-2 of the Law of 5 April 1993, as amended. Whilst, the MiFID II Delegated Regulation is directly applicable in Luxembourg since January 3, 2018, without the need for any national implementing act.

In addition, the EBA Guidelines and Outsourcing Circulars should be adhered to by the obliged entities, to the extent applicable.

Article 37-1 (5) of the Law of 5 April 1993 on the financial sector, as amended, elaborates further on the organisational requirements applicable to credit institutions and investment firms, when entering into an outsourcing arrangement. Such provisions include:

- Outsourcings shall not impair the level and quality of service towards the clients and shall be based on a service level agreement;
- Credit institutions and investment firms shall remain fully responsible to ensure compliance with all of their obligations pursuant to applicable prudential regulation;
- Credit institutions and investment firms shall take reasonable measures in order to avoid an excessive increase of operational risks; and
- credit institutions and investment firms shall have in place strong security mechanisms that guarantee the security and authentication of the means through which information is transferred, reduce the risk of data corruption and unauthorised access and prevent information leakage in order to maintain, at all times, confidentiality of data.

No additional rules or guidance on outsourcing within the context of MiFID II have been published by the Luxembourg national authorities.

## GDPR and NIS Directive

The GDPR has been directly applicable in Luxembourg since May 25, 2018, without the need for any national implementing act. Nevertheless, Luxembourg has enacted the following two data protection laws of 1 August 2018 complementing the GDPR:

- The Law on the organisation of the National Data Protection Commission and the general data protection framework (repealing the previous Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data, as amended); and
- The Law on the protection of individuals with regard to the processing of personal data in criminal matters as well as in matters of national security.

The new legislative framework amends the Luxembourg Labour Code and the Law of 25 March 2015 laying down the system of salaries and the conditions and procedures for advancement of civil servants of the State, as amended.

The NIS Directive was fully transposed into Luxembourg Law with the implementation of the Luxembourg Law of 28 May 2019.

No additional rules or guidance on outsourcing within the context of GDPR or NIS Directive have been published by the Luxembourg national authorities.

## CRD IV

The CRD IV was fully transposed into Luxembourg Law with the implementation of the Luxembourg Law of 2 July 2015 by amending the Law of 5 April 1993 on the financial sector, to the extent necessary. The implementation of the CRD IV legislative package in Luxembourg is also accompanied by the following CSSF regulations:

- CSSF Regulation N° 18-03 (i) implementing certain discretions of Regulation (EU) No 575/2013 and implementing Guideline (EU) 2017/697 of the European Central Bank of 4 April 2017 on the exercise of options and discretions available in Union law by national competent authorities in relation to less significant institutions (ECB/2017/9) and (ii) repealing CSSF Regulation N° 14-01;
- CSSF Regulation N° 15-01 on the calculation of institution-specific countercyclical capital buffer rates, transposing Article 140 of Directive 2013/36/EU; and
- CSSF Regulation N° 15-02 relating to the supervisory review and evaluation process that applies to CRR institutions.

Articles 36-2 and 37-1 (5) of the Law of 5 April 1993 on the financial sector also apply to credit institutions subject to CRD IV.

The EBA Guidelines and Outsourcing Circulars should be adhered to by the obliged entities, to the extent applicable. No additional rules or guidance on outsourcing within the context of CRD IV have been published by the Luxembourg national authorities.

## The MLD

The Law of 13 February 2018 partially transposed the MLD into Luxembourg law by amending:

- Law of 12 November 2004 on the fight against money laundering and terrorist financing;
- Law of 10 November 2009 on payment services;
- Law of 9 December 1976 on the organisation of the profession of notary;
- Law of 4 December 1990 on the organisation of bailiffs (huissiers de justice);
- Law of 10 August 1991 on the legal profession;
- Law of 5 April 1993 on the financial sector;
- Law of 10 June 1999 on the organisation of the accounting profession;
- Law of 21 December 2012 in relation to the Family Office activity;
- Law of 7 December 2015 on the insurance sector; and
- Law of 23 July 2016 concerning the audit profession.

The Law of 13 February 2018 is closely connected with the Law of 13 January 2019 which established a register of beneficial owners, effectively transposing Articles 30 and 31 of the MLD.

Along with the above-mentioned transposing legislation, the CSSF published the following guidance complementing the anti-money laundering and terrorist financing legislative framework in Luxembourg:

- CSSF Circular 18/684 regarding the entry into force of the law of 13 February 2018 amending, inter alia, the Law of 12 November 2004 on the fight against money laundering and terrorist financing; and
- CSSF Regulation N° 12-02 of 14 December 2012 on the fight against money laundering and terrorist financing.

It should be noted that Article 37 of the CSSF Regulation N° 12-02 is more explicit compared to Article 29 of the MLD on the contractual requirements between the obliged entity and the third party in the context of outsourcing or agency relationships.

Within the context of outsourcing, the MLD merely states that (reiterating para. 36 – preamble): “In the case of agency or outsourcing relationships on a contractual basis between obliged entities and external persons not covered by this Directive, any AML/CFT obligations upon those agents or outsourcing service providers as part of the obliged entities could arise only from the contract between the parties and not from this Directive. Therefore the responsibility for complying with this Directive should remain primarily with the obliged entity.”

The MLD does not specify any minimum requirements as to the content and format of such contract, or what steps a supervised entity should take prior to outsourcing any of its AML functions as permitted by the Directive. In contrast, Article 37 of the CSSF Regulation N° 12-02 requires entities which are subject to the CSSF’s supervision on AML matters to include the following within the context of outsourcing or agency relationships:

- a detailed description of the due diligence measures and procedures to be implemented in accordance with the Luxembourg AML Law and relevant national regulations and, in particular, of the information and documents to be requested and verified by the third-party representative; and
- the conditions regarding the transmission of information to the supervised entity, including, to make available immediately, regardless of confidentiality or professional secrecy rules or any other obstacle, the information gathered while fulfilling the customer due diligence obligations and the transmission, upon request and without delay, of a copy of the original supporting evidence received in this respect.

The CSSF Regulation N° 12-02 further requires that the internal procedures of the supervised entity wishing to use third parties for outsourcing or agency relationships shall include detailed provisions on the procedures to apply when using a third-party representative, as well as the relevant criteria determining the choice of this third-party representative. The supervised entity shall carry out a regular control of compliance by the third-party representative with the commitments arising from the contract.

No additional rules or guidance on outsourcing within the context of the MLD have been published by the Luxembourg national authorities.

## BMR

The BMR has been directly applicable in Luxembourg since 1 January 2018, without the need for any national implementing act. Nonetheless, Luxembourg enacted the Law of 17 April 2018 on indices used as benchmarks in the context of financial instruments and contracts or for measuring performance investment funds, adopting BMR in Luxembourg and amending:

- the Luxembourg Consumer Code;
- the Law of 23 December 1998 establishing a financial sector supervisory committee;
- the Law of 12 November 2004 on the fight against money laundering and the financing of terrorism; and
- the Law of 7 December 2015 on the insurance sector.

No additional rules or guidance on outsourcing within the context of BMR have been published by the Luxembourg national authorities.

**ESMA Guidelines on certain aspects of MiFID compliance function requirements (28 September 2012) (2012/388)**

The CSSF Circular 12/552 adopts the ESMA Guidelines (para. 6.2.6).



# Spain

## Regulatory approach

Outsourcing is becoming a key area of focus for the Spanish regulators (i.e., the Bank of Spain, the Spanish Securities Market Commission (the “CNMV”) and the General Directorate for Insurance and Pension Funds (the “DGSFP”), together the “**Spanish Regulators**”), particularly in light of its importance in the context of operational resilience and the stability of Spanish firms and the Spanish markets. Consequently, Spanish regulated firms intending to outsource need to be aware of the Spanish regulators’ expectations in this regard.

The outsourcing criteria applicable to Spanish firms is set out by the laws applicable to each type of financial institution. As such, this section is formatted to address each type of institution separately:

- Credit entities, which are subject to, among others:
  - Law 10/2014 of 26 June 2014 on the organisation, supervision and solvency of credit entities (the “**Spanish Credit Entities Law**”);
  - Royal Decree 84/2015 of 13 February implementing the Spanish Credit Entities Law (the “**Spanish Credit Entities Regulation**”); and
  - the Circular of the Bank of Spain 2/2016 of 2 February to credit entities on supervision and solvency, which completes the implementation in Spanish law of Directive 2013/36/EU and Regulation (EU) no. 575/2013 (“**Circular 2/2016**”).
- Investment firms, which are subject to, among others:
  - Royal Legislative Decree 4/2015 of 23 October 2015, approving the revised text of the Securities Market Law (the “**Spanish Securities Market Law**”);
  - Royal Decree 217/2008 of 15 February 2008 on the legal regime for investment services firms and other entities providing investment services (the “**Spanish Investment Firms Regulation**”); and
  - the “*Questions and Answers intended for FinTech companies on activities and services that may be related to the CNMV*” (the “**Fintech Q&A**”).
- Payment institutions, which are subject to, among others:
  - Royal Decree-Law 19/2018 of 23 November 2018 on payment services and other urgent financial measures (the “**Spanish Payment Services Law**”); and
  - Royal Decree 736/2019 of 20 December 2019 on the legal regime for payment services and payment institutions (the “**Spanish Payment Services Regulation**”).
- Electronic money institutions, which are subject to, among others:
  - Law 21/2011 of 26 July 2011 on electronic money (the “**Spanish Electronic Money Law**”); and
  - Royal Decree 778/2012 of 4 May 2012 on the legal regime for electronic money institutions (the “**Spanish Electronic Money Regulation**”).
- Insurance and reinsurance entities, which are subject to, among others:
  - Law 20/2015 of 14 July 2015 on the organisation, supervision and solvency of insurance and reinsurance companies (the “**Spanish Insurance Companies Law**”), and
  - Royal Decree 1060/2015 of 20 November on the organisation, supervision and solvency of insurance and reinsurance companies (the “**Spanish Insurance Companies Regulation**”).

As a general remark, these outsourcing requirements have not been subject to further analysis from the regulators in their publications, aside from in: (i) Circular 2/2016; and (ii) the Fintech Q&A.

Additionally, the Bank of Spain adheres to the EBA Guidelines, as discussed at Part One, on outsourcing agreements and has agreed to comply with such rules by 30 September 2019, with a few exceptions. On 25 February 2019, the EBA published a “Guidelines compliance table”<sup>10</sup> which details whether the competent authorities of each Member State intend to comply with the EBA Guidelines on outsourcing agreements (the “**EBA Guidelines Compliance Table**”). In this document, the Bank of Spain declared that it did not intend to comply with certain EBA Guidelines, which we explain in detail, below.

## Outsourcing requirements applicable to Spanish credit entities

According to the Spanish Credit Entities Regulation, credit entities may delegate the provision of operational activities to a third party, provided that: (i) the outsourcing does not remove the substance from the credit entity to render it an empty shell; and (ii) the delegation does not undermine the internal control capabilities of the entity itself or the supervisory capabilities of the Bank of Spain and the European Central Bank.

<sup>10</sup> EBA, 25 February 2020, “Guidelines compliance table”, available at:

[https://eba.europa.eu/sites/default/documents/files/document\\_library/875334/EBA%20GL%202019%2002%20-%20%20CT%20GLs%20on%20outsourcing%20arrangements.pdf](https://eba.europa.eu/sites/default/documents/files/document_library/875334/EBA%20GL%202019%2002%20-%20%20CT%20GLs%20on%20outsourcing%20arrangements.pdf)



Article 22 of the Spanish Credit Entities Regulation and Article 43 of Circular 2/2016 set out the following requirements applicable to the outsourcing of operational activities by credit entities:

### What operational activities can be outsourced?

Activities reserved to credit entities (i.e., the raising of repayable funds from the public for whatever purpose in the form of deposits, loans, repurchase agreements or similar instruments) may not be delegated, except in cases where the delegation is made in favour of an agent of the credit entity, which is subject to the following limitations:

- Agents may not formalise guarantees, warranties or other risks on behalf of the credit entity; and
- Where the agency agreement provides for the receipt or delivery to the agent of funds in cash, cheques or other payment instruments, these may not be paid to the agent or drawn from the agent's bank accounts.

Please note, the above answer materially differs from the EBA Guidelines. Pursuant to guidelines 62 and 63 of the EBA Guidelines, institutions are able to outsource any function of banking activities or payment services, as long as: (i) the service provider is authorised or registered by a competent authority to perform such banking activities or payment services; or (ii) the service provider is otherwise allowed to carry out those banking activities or payment services in accordance with the relevant national legal framework.

The Bank of Spain has declared in the EBA Guidelines Compliance Table its intention to comply with the EBA Guidelines, with the exceptions of Guidelines 62 and 63, when they relate to the outsourcing of functions of banking activities that consist of taking deposits or other activities that involve repaying public funds. With respect to the outsourcing of functions of banking services, the Bank of Spain considers Guidelines 62 and 63 to be inconsistent with the Spanish national provisions implementing CRD IV and will therefore not comply with them. Particularly, Article 22 of the Spanish Credit Entities Regulation sets out that activities reserved for credit entities (i.e., taking deposits or other activities that involve repaying public funds) cannot be outsourced. However, the outsourcing of mere operational functions is allowed (i.e., cloud storage services; IT, cybersecurity and software services; KYC services; file management services; back office services; the processing, management and shipping of credit cards; telephone banking services; customer services; and complaints/incident management services), subject to the requirements set out below.

### What operational activities are deemed essential for the purposes of outsourcing?

A function or service shall be deemed to be essential for a credit entity if a deficiency or abnormality in its performance is likely to significantly affect the credit entity's ability to permanently comply with the conditions and obligations arising from its authorisation and from the provisions set out in the Spanish Credit Entities Law, or to affect its financial performance, solvency or continuity of business.

What are the requirements to outsourcing activities?

Article 43 of Circular 2/2016 sets out that credit entities that have outsourced operational activities, including within the credit entity's group itself, must put in place a delegation policy, which is approved by their board of directors and subject to express periodic updates to be carried out at least every two years. Additionally, the credit entity shall specify the area control unit or service receiver responsible for the monitoring and control of any of the delegated functions or services.

When selecting service providers, credit entities must assess (among other factors that may be relevant in each case) the quality, experience and stability of the providers and the degree to which they comply with the most relevant laws and regulations applicable to them, regardless of whether the activity to be outsourced is deemed essential or not. In particular, they must assess the way in which the anti-money laundering prevention and customer protection regulations are complied with.

Furthermore, outsourcing of essential functions or services shall comply with the following additional requirements:

- Under no circumstances shall the outsourcing of the essential function or service imply a transfer of responsibility by senior management. In particular, the delegation may not reduce the requirements applicable to internal control mechanisms;
- Outsourcing may not alter the relations and obligations of the credit entity vis-à-vis its clients or with the authority competent for its supervision;
- The conditions to be met by the credit entity in order to receive and retain authorisation may not be waived or amended due to the existence of an outsourcing agreement; and
- The outsourcing agreement between the credit entity and the third party must be set out in a written contract specifying the rights and obligations of the parties.

Under the delegation policy set out in Circular 2/2016, the credit entity must evaluate the potential impact of any risks it incurs and specify to the management that it will assess these risks in accordance with their materiality. At the very least, in relation to the delegation of essential services and functions, the following should be considered:

- The risk of non-compliance with the rules that regulate the entity's activity and with the most relevant rules that apply to the service provider;
- The risk of concentration arising from the accumulation of services or functions delegated to the same supplier or to the same geographical area;
- The risk inherent in the country in which the service provider is based;
- Reputational risk arising from the service provider's practices that could generate a negative opinion of an institution by its customers, investors, the supervisor or the market in general; and

- The operational risk, including legal risk, due to failures in the provision of the service by the provider, as a result of, among other factors, the inadequacy of the processes, internal systems or assigned personnel.

In relation to outsourcing of essential functions, the board of directors shall ensure that the requirements set out in its policy regarding the delegation of services or functions are met through the receipt of monitoring reports, prepared by the relevant internal department. Internal audit shall review the content of these reports, which may vary in frequency and depth depending on the nature or criticality of the services or functions delegated, but shall assess both the risks and the benefits obtained from the delegation and shall be updated at least annually.

Outsourcing of essential functions must not hinder the supervisory powers of the competent authority or make the entity excessively dependent on the service provider. To this end, outsourcing agreements must:

- Include a clause providing for direct and unrestricted access by the competent authority to the relevant information held by the suppliers, as well as the possibility of verifying, on the suppliers' own premises, the suitability of the systems, tools or applications used in the provision of the delegated services or functions;
- Allow for termination and ensure that the costs of such termination are reasonable;
- Allow the entity to limit the sub-contracting of services by the service provider and/or extend the principles of entity's delegation policy to outsourced services;
- Include a requirement for the service provider to have a contingency plan to maintain its activity and limit the entity's losses in the event of any serious incident; and
- If the supplier is based abroad a clause must be included specifying the jurisdiction of the country to which the contract will be subject, so that the entity is aware of the potential legal risks it may incur in the event of a conflict or breach.

Credit entities shall ensure that their own contingency plans adequately provide for the services or functions that have been outsourced, in particular those of an essential nature, and shall establish alternatives to the agreed outsourcing.

#### **Does the Bank of Spain authorise the outsourcing of important operational functions?**

Institutions shall formally communicate to the competent authority, at least one month in advance, their plans for the outsourcing of essential functions or services. Such communication shall be accompanied by the relevant risk analysis and mitigation measures, if any, especially when the outsourcing involves the use of new technologies.

Depending on the nature or criticality of certain functions or services, or their effects on the credit entity's internal governance system, the competent authority may establish limitations to the outsourcing. In making its decision, the competent authority shall take into account, among other factors, the entity's established delegation policy, its organisational structure, its internal control environment and the implications of the delegation for the exercise of the competent authority's supervisory function.

#### **Who bears the responsibility for the outsourced functions?**

The credit entities. Outsourcing of operational activities or functions by credit entities to third parties does not reduce the credit entities' responsibility for the full performance of its obligations.

### **Outsourcing requirements applicable to Spanish investment firms**

The Spanish Securities Market Law, together with the Spanish Investment Firms Regulation, sets out the following requirements applicable to the outsourcing of operational activities by investment firms.

#### **What are the requirements to outsourcing activities?**

In accordance with Articles 30 to 32 of the MiFID II Delegated Regulation, explained in Part Two, when outsourcing operational functions which are crucial or important for the provision of continuous and satisfactory service to clients and the performance of investment activities on a continuous and satisfactory basis, investment firms shall ensure that they take reasonable steps to avoid undue additional operational risk.

Outsourcing of crucial or important operational functions must not materially affect the quality of internal controls or the ability of the regulator to monitor the investment firm's compliance with all its obligations.

Article 30 of the Spanish Investment Firms Regulation states that every investment firm must have adequate administrative and accounting procedures, internal control mechanisms, effective risk assessment techniques and efficient control and safeguard mechanisms for its IT systems, which shall be governed by articles 23 and 24 of MiFID II Delegated Regulation, explained in Part Two.

The investment firm must have strong security mechanisms in place to ensure the security and authentication of the means of transmission of information, to minimise the risk of data corruption and unauthorised access and to prevent leakage of information, while maintaining the confidentiality of data.

#### **Does CNMV authorise the outsourcing of important operational functions?**

Article 30 of the Spanish Investment Firms Regulation cross references article 31(5) of the MiFID II Delegated Regulation, under which investment firms must, on request by the competent authority, make available all information necessary to enable the authority to supervise compliance with the requirements of MiFID II and its implementing regulations, in relation to the performance of outsourced functions.

The CNMV has confirmed that investment firms do not have to submit any underlying documentation to the CNMV prior to carrying out an outsourcing. However, the CNMV may subsequently request this documentation during an on-site inspection or by virtue of an information request in the context of an investigation.

Article 285 of the Spanish Securities Market Law states that investment firms must not outsource investment services functions when this diminishes internal controls or the supervisory capacity of the CNMV.

### **Who bears the responsibility for the outsourced functions?**

According to article 31(1) of MiFID II Delegated Regulation, investment firms outsourcing critical or important operational functions shall remain fully responsible for discharging all of their obligations under MiFID II.

### **Rules relating to certain specific investment firm vehicles**

- Outsourcing requirements set out in the CNMV Fintech Q&A
- On 12 March 2019, the CNMV uploaded the latest version of its Fintech Q&A, a document which is not binding in nature, but nonetheless provides a set of guidelines aimed at entities wishing to operate in the FinTech field, which includes a set of interpretation criteria for the proper implementation of the securities market rules. The Fintech Q&A is a work in progress and is updated regularly, as and when the CNMV gains knowledge of the latest trends applicable to FinTech companies.
- On the basis of the Fintech Q&A, the CNMV analyses the nature of the activities carried out by companies that act as technology providers for investment firms or other entities registered with the CNMV, determining whether those companies require regulatory approval in order to carry out their services. If the outsourced technology services include the outsourcing of critical or important operational functions of the investment firm or of any other entity registered with the CNMV, the technology provider must cooperate with the competent authority in order to facilitate their supervision.
- This requirement applies to the outsourcing of functions by investment firms, which are supervised by the CNMV. In practical terms, this requirement to cooperate should be set out in the outsourcing agreement to be entered into by the investment firm and the third-party provider, as an obligation applicable to the service provider.
- Outsourcing requirements set out in the Spanish Securities Market Law for data-provision service providers
- According to the Spanish Securities Market Law, where a data-provision service provider outsources certain activities on its behalf, including to companies with which it has close links, it must ensure that the third party service provider has the powers and ability to carry out the activities in a reliable and professional manner.
- Article 197 of the Spanish Securities Market Law states that the providers of data supply services must inform the CNMV about outsourcing of functions. Prior to outsourcing, data supply service providers must provide the CNMV with information specifying which activities are to be outsourced, indicating the human and technical resources required to perform each of the activities.

## **Outsourcing requirements applicable to Spanish payment institutions**

Pursuant to the provisions of the Spanish Payment Services Law, any outsourcing of operational functions made by a payment institution must be disclosed to the Bank of Spain (irrespective of whether such operational functions are considered essential or not). Spanish payment institutions are allowed to outsource “important operational functions”, including IT systems, as long as the outsourcing does not significantly affect either the quality of the payment institution’s internal control measures or the ability of the regulator to control and monitor the compliance with its applicable regulations. Regardless of the activity outsourced, the control or monitoring of applicable regulations is ensured by the payment institution through the inclusion of protective language in the services agreements which may consist of one or more of the following undertakings:

- the cooperation by the parties upon a regulatory request or investigation;
- allowing on-site inspections by the client or the regulatory authority (as the case may be) at the services provider’s premises to guarantee compliance with applicable laws; or
- the client may audit the level of services provided by the services provider from time to time and request adjustments if necessary.

The Spanish Payment Services Regulation sets out in article 15 the following requirements applicable to the outsourcing of operational functions by payment institutions.

### **To whom are these requirements applicable?**

These requirements apply to payment institutions that outsource functions to a third party or to an entity which belongs to the same group as the payment entity. Outsourcing includes both the delegation of functions to a third party, as well as any subsequent delegation by such third party.

### **What operational activities are deemed important for the purposes of outsourcing?**

An operational function shall be deemed important for the purposes of these requirements if an anomaly or deficiency in its execution may substantially affect the entity’s capacity to permanently fulfil its regulatory obligations, or affect the financial results, soundness or continuity of its payment services or the confidentiality of the information the entity deals with.

## What are the limits to outsourcing activities?

Outsourcing of important functions shall not: (i) remove the substance from the credit entity to render it an empty shell; (ii) significantly affect the quality of the institution's internal control measures; or (iii) undermine the Bank of Spain's supervisory powers over the functions that the payment institution performs through its third-party suppliers.

In particular, when important operational functions are outsourced, the following apply:

- The outsourcing shall not include the assignment of responsibilities of senior management;
- The relationships and obligations of the institution in accordance with current legislation vis-à-vis its users or the Bank of Spain shall not be altered as a consequence of the outsourcing;
- The outsourcing shall not undermine the conditions and requirements that the payment institution must fulfil in order to retain its regulatory authorisation nor shall it lead to the removal or modification of any of the other conditions to which the payment institution's authorisation has been subject; and
- Any outsourcing agreement must be set out in written form. The agreement shall include a clause providing for direct and unrestricted access by the payment institution and the Bank of Spain to any of the institution's information held by the third party, as well as the possibility of verifying, on the third party's own premises, the suitability of the systems, tools or applications used in the provision of outsourced functions. In addition, if the third party is based abroad, a clause must be included specifying the jurisdiction of the country to which the contract will be subject, so that the entity is aware of the potential legal risks it may incur in the event of a conflict.

## Does the Bank of Spain authorise the outsourcing of important operational functions?

The outsourcing of important payment services functions (or any changes to already existing outsourcing of functions), including changes in the IT systems, must be communicated to the Bank of Spain at least one month prior to the adoption of the measures or the effective outsourcing. Within one month from receiving the communication, the Bank of Spain may, giving reasons, impose limitations to the outsourcing or oppose the outsourcing altogether when the aforementioned requirements are not met.

The outsourcing of non-important payment services functions must be communicated to the Bank of Spain at least one (1) month prior to the adoption of the measure or the effective outsourcing, but will not be subject to opposition from the Bank of Spain.

## Who bears the responsibility for the outsourced functions?

Notwithstanding the outsourcing of its operational activities, the Spanish Payment Services Law states that payment institutions shall remain fully responsible for the actions arising from the outsourced activities.

## Can Spanish payment institutions outsource core regulated services or functions?

Pursuant to Guideline 62 of the EBA Guidelines, payment institutions should ensure that the outsourcing of payment services functions, to the extent that the performance of that function requires authorisation or registration by a competent authority in the Member State where they are authorised, to a service provider located 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 otherwise allowed to carry out those banking activities or payment services in accordance with the relevant national legal framework. However, the Bank of Spain has declared that the Spanish legal framework shall not use the condition at Guideline 62(b), but rather only the one set out in Guideline 62(a) (i.e., the service is authorised or registered by a competent authority to perform such payment services).

The Spanish Payment Services Regulation has granted specific regulatory powers to the Bank of Spain to further develop the requirements applicable to the outsourcing of important operational functions by payment institutions. In particular, the Bank of Spain has powers to regulate: (i) the criteria to determine when an agreement shall be considered outsourcing; (ii) the criteria to determine when a function may be deemed an important operational function; (iii) the rules that apply to the process of outsourcing; and (iv) the minimum content that must be included in the communications to the Bank of Spain.

The Bank of Spain has confirmed that, as of 6 March 2020, it has not acted to regulate outsourcing by payment institutions any further. Furthermore, there is no indication that any additional criteria will be implemented by the Bank of Spain in the near future.

## Outsourcing requirements applicable to Spanish electronic money institutions

Pursuant to the provisions of the Spanish Electronic Money Law, electronic money institutions may delegate the performance of certain activities, such as the provision of operational functions or the distribution and redemption of electronic money, to third parties. However, the Spanish Electronic Money Law provides a prohibition on issuing electronic money through agents.

Any outsourcing of operational functions made by an electronic money institution must comply with the requirements set out in the Spanish Electronic Money Regulation and any other implementing regulations.



Article 15 of the Spanish Electronic Money Regulation sets out the same requirements for the outsourcing of operational functions by electronic money institutions as to those applicable to the outsourcing of operational functions by payment institutions discussed above.

#### **Who are these requirements applicable to?**

These requirements apply to the outsourcing of functions to a third party or to an entity which belongs to the same group as the electronic money institution. Additionally, outsourcing includes both the delegation of functions to a third party, as well as any subsequent delegations by such third party.

#### **What operational activities are deemed important for the purposes of outsourcing?**

An operational function shall be deemed important for the purposes of these requirements if an anomaly or deficiency in its execution may substantially affect the entity's capacity to permanently fulfil its regulatory obligations, or affect the financial results, soundness or continuity of its services or the confidentiality of the information the entity deals with.

#### **What are the limits to outsourcing activities?**

Outsourcing of important functions shall not: (i) remove the substance from the credit entity to render it an empty shell; (ii) significantly affect the quality of the institution's internal control measures; or (iii) undermine the Bank of Spain's supervisory powers over the functions that the electronic money institution performs through its third-party suppliers.

In particular, when important operational functions are outsourced, the following apply:

- The outsourcing shall not include the assignment of responsibilities of senior management;
- The relationships and obligations of the institution in accordance with current legislation vis-à-vis its users or the Bank of Spain shall not be altered as a consequence of the outsourcing;
- The outsourcing shall not undermine the conditions and requirements that the electronic money institution must fulfil in order to retain its regulatory authorisation nor shall it lead to the removal or modification of any of the other conditions to which the electronic money institution's authorisation has been subject; and
- Any outsourcing agreement must be set out in written form. The agreement shall include a clause providing for direct and unrestricted access by the electronic money institution and the Bank of Spain to any of the institution's information held by the third party, as well as the possibility of verifying, on the third party's own premises, the suitability of the systems, tools or applications used in the provision of outsourced functions. In addition, if the third party is based abroad, a clause must be included specifying the jurisdiction of the country to which the contract will be subject, so that the entity is aware of the potential legal risks it may incur in the event of a conflict.

#### **Does the Bank of Spain authorise the outsourcing of important operational functions?**

The outsourcing of important functions relating to the issuance of electronic money or the granting of payment services (or any changes to an already existing outsourcing of functions), including changes in the IT systems, must be communicated to the Bank of Spain at least one month prior to the adoption of the measure or the effective outsourcing. Within one month from receiving the communication, the Bank of Spain may, giving reasons, impose limitations to the outsourcing or oppose the outsourcing altogether when the aforementioned requirements are not met.

The outsourcing of non-important functions of services must be communicated to the Bank of Spain at least one month prior to the adoption of the measure or the effective outsourcing, but will not be subject to opposition from the Bank of Spain.

#### **Who bears the responsibility for the outsourced functions?**

Notwithstanding the outsourcing of its operational activities, the Spanish Electronic Money Law sets out that electronic money institutions shall be fully responsible for the actions arising from the outsourced activities.

The Spanish Electronic Money Regulation has granted specific regulatory powers to the Bank of Spain to further develop the requirements applicable to the outsourcing of important operational functions by electronic money institutions. In particular, the Bank of Spain has powers to regulate: (i) the criteria to determine when an agreement shall be considered outsourcing; (ii) the criteria to determine when a function may be deemed an important operational function; (iii) the rules that apply to the process of outsourcing; and (iv) the minimum content that must be included in the communications to the Bank of Spain.

The Bank of Spain has confirmed that, as of 6 March 2020, it has not regulated outsourcings by electronic money institutions any further. Furthermore, there is no indication that any additional criteria will be implemented by the Bank of Spain in the near future.



## Outsourcing requirements applicable to Spanish insurance and reinsurance entities

Article 13.3 of the Spanish Insurance Companies Law sets out that any type of arrangement entered into between an insurance or reinsurance company and a third party, regardless of whether the third party is a supervised entity, whereby the latter performs, directly or by way of subcontracting, an activity or function which would otherwise have been performed by the insurance or reinsurance company by itself shall be deemed as the outsourcing of functions of an insurance or reinsurance company.

### What are the requirements to outsourcing activities?

Article 44.2 of the Spanish Insurance Companies Regulation sets out that insurance and reinsurance companies shall have implemented written policies concerning at least risk management, internal controls and audit, and, where appropriate, outsourcing of functions or activities.

The written policies shall be approved by the company's board of directors, reviewed at least annually and be adapted to significant changes in the system or area relative to the function concerned.

Article 164 of the Spanish Insurance Companies Regulation specifies that in case of outsourcing of an insurance or reinsurance function or activity, the service provider shall collaborate with the DGSFP in relation to the supervision of the outsourced function or activity and shall provide the information required in relation to such functions or activities to the DGSFP, as well as to the insurance or reinsurance companies themselves and their auditors. The insurance and reinsurance entities that outsource functions or activities shall adopt the necessary measures to ensure that information and access obligations are met by the person providing the outsourced service.

If the activities outsourced are deemed critical or important functions, the insurance or reinsurance company in question must appoint a person inside the company who will be responsible for the outsourced function or activity, with sufficient experience and knowledge to be able to monitor the performance of the external service providers.

### What are the limits to outsourcing important or critical activities?

Insurance or reinsurance companies may outsource critical or important operational functions or activities except under the following circumstances:

- if the quality of their governance systems is significantly undermined by the outsourcing of functions; or
- if the outsourcing: (i) increases operational risk; (ii) undermines the DGSFP's supervisory powers over the functions carried out by the insurance and reinsurance companies; or (iii) affects the continuous and satisfactory service granted by the insurance or reinsurance company to the policyholders.

### Does the DGSFP authorise the outsourcing of functions?

The outsourcing of important or critical functions or activities by insurance and reinsurance companies (or any significant change to an already existing outsourcing of functions), must be communicated to the DGSFP prior to carrying out the outsourcing. Within one month from receiving the communication, the DGSFP may oppose the outsourcing when the aforementioned requirements are not met.

For the purposes of the outsourcing mentioned above, any changes regarding the person responsible for the function, changes in the service provider or changes to the scope of the outsourced activities shall be deemed significant.

### Over whom does the DGSFP have supervisory powers regarding the outsourcing of activities?

Pursuant to article 122 et seq. of the Spanish Insurance Companies Law, providers of outsourced functions are subject to the supervision of the DGSFP. In this regard, the DGSFP is authorised to carry out its inspection powers in the premises of the service providers which carry out the outsourced functions. If the premises of the outsourced service provider are located in another Member State, the DGSFP shall carry out the supervisory actions on those premises, either itself or through the intermediary or persons it designates, after informing the competent authorities of that Member State. If the person providing the service is not subject to a specific supervisory regime, the insurance supervisory authorities of that Member State shall be informed. The DGSFP may delegate the carrying out of such actions to the supervisory authorities of the Member State where the service provider is located, if agreed between the two authorities.

Moreover, the Spanish Insurance Companies Law sets out that the DGSFP is authorised to implement certain special control measures if the outsourcing of activities entails relevant deficiencies in the governance and internal control systems of the insurance or reinsurance company. Special control measures include, among others, the implementation of a short-term financing plan or a recovery plan, limitations to the disposal of assets and the suspension of the undertaking of any additional insurance agreements.

### Who bears the responsibility for the outsourced functions?

Notwithstanding the outsourcing of its operational activities, the Spanish Insurance Companies Law sets out that the insurance and reinsurance companies shall remain fully responsible for the actions arising from their outsourced activities.

# United Kingdom

## Regulatory approach

Outsourcing remains a key area of focus for UK regulators, in particular in light of its importance in the context of operational resilience and the stability of UK firms and the UK markets. Consequently, UK regulated firms intending to outsource need to be aware of the UK regulators' expectations in this regard. It is important to note that an EEA firm that does not have (or does not wish to exercise) a treaty right to carry on a particular regulated activity in the UK must seek Part 4A permission ("**Top-up Permission**") from the Prudential Regulation Authority (the "**PRA**") or Financial Conduct Authority ("**FCA**"). Under this arrangement the EEA firm in question would then be regulated by the PRA or FCA for the activities it is authorised for under the Top-Up Permission, thereby subjecting it to the UK outsourcing regimes and supervision. This is distinct from a situation where an EU firm performs regulated activities in the UK under a treaty right and is not regulated by the UK regulators (for example, a UK branch of an EEA firm, which performs regulated activities solely through its passporting rights).

On 5 December 2019, the Bank of England ("**BOE**") and the PRA published a consultation paper on outsourcing and third party risk management<sup>11</sup> ("**CP30/19**"). The PRA is consulting on a new Supervisory Statement to help modernise the regulatory framework in this area, the key objectives of which are to complement the PRA's policy proposals on operational resilience, implement key EU guidance (including the EBA Guidelines) by clarifying precise expectations and to facilitate greater resilience and adoption of the cloud and other new technologies.

CP30/19 was published alongside a shared policy summary and co-ordinated consultation papers from the BOE, the PRA and the FCA on new requirements to strengthen operational resilience in the financial services sector ("**Shared Operational Resilience Policy**").<sup>12</sup> As part of these proposals outsourcing is highlighted as one of the supporting requirements to the PRA's operational resilience policy.<sup>13</sup> In addition, the operational resilience proposals expressly cross-refer to CP30/19, noting that the proposals in this consultation include provisions which are relevant to firms' operational resilience. The FCA has also emphasised that it is particularly concerned that outsourcing by investment firms may contribute to a greater threat to stability and resilience due to reduced direct oversight.<sup>14</sup> Accordingly, there is currently a particular focus on outsourcing by all of the UK regulators, both directly and also in the wider context of operational resilience.

The FCA introduced guidance for firms outsourcing to the cloud and other third-party IT services in 2006,<sup>15</sup> which preceded any EU guidance in this area. When the EBA Guidelines were created, the FCA modified its guidelines so that they only apply to firms that are outside the scope of the EBA Guidelines. Firms within scope of the EBA Guidelines are expected to apply the EBA Guidelines.

As stated above, the default position of the UK regulators on outsourcing is the EU-wide position stated in Parts One and Two. Nonetheless, there are several UK-specific regulatory considerations concerning outsourcing, which firms must be aware of and compliant with in addition to the EU requirements when deciding to outsource services, as outlined below.

## FCA Principles for Businesses (The "FCA Principles")

The FCA Principles are general statements of the fundamental obligations of authorised firms and the other persons to whom they apply under the regulatory system. They derive their authority from the FCA's rule-making powers. The FCA Principles apply to all FCA regulated firms and provide a basis for FCA supervision and enforcement. This means that firms can be the subject of disciplinary measures if they have breached an FCA Principle without breaking any other specific FCA rule. The FCA has used the FCA Principles as the basis of its recent enforcement actions in relation to outsourcing. As a result, firms must consider the application of the FCA Principles to their outsourcing activities. For an explanation of how the FCA Principles apply to outsourcing arrangements please see Schedule 4.

## PRA Fundamental Rules (The "PRA Principles")

The PRA Principles act collectively as an expression of the PRA's general objective of promoting the safety and soundness of PRA regulated firms. The PRA is responsible for the prudential regulation and supervision of around 1,500 banks, building societies, credit unions, insurers and major investment firms. These entities are typically viewed as the most systemically important financial institutions in the UK, and, consequently, they are subject to regulation by both the PRA and the FCA. There are eight PRA Principles and they each apply to every PRA-authorised firm in parallel with the FCA Principles. Similar to the FCA Principles, the PRA Principles often form the

---

<sup>11</sup> CP30/19 Outsourcing and third party risk management (December 2019)

<sup>12</sup> CP29/19 (PRA), CP19/32 (FCA) and BOE CP - Building operational resilience: Impact tolerances for important business services

<sup>13</sup> CP29/19 Operational resilience: Impact tolerances for important business services (December 2019)

<sup>14</sup> FCA, January 2019, "Sector Views", available at: <<https://www.fca.org.uk/publication/corporate/sector-views-january-2019.pdf>>

<sup>15</sup> FCA, July 2016 (updated September 2019), "FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services", available at: <<https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf>>.

basis for PRA supervision and enforcement. Firms can, therefore, be the subject of disciplinary measures if they have breached a PRA Principle without breaking any other specific rule. The PRA has used the PRA Principles as the basis of its recent enforcement actions in relation to outsourcing. As a result, PRA-regulated firms must consider the application of the PRA Principles to their outsourcing activities. For an explanation of how the PRA Principles apply to outsourcing arrangements, please see Schedule 4.

## CP30/19 – Outsourcing and third party risk management

In CP30/19, the PRA set out and invited comments on its proposals on modernising the legal framework surrounding outsourcing and third-party risk management. The proposals are contained in a draft supervisory statement (“**Draft SS**”) within CP30/19. Please note, the proposals may change following the public consultation, therefore, the content of this section may also be subject to change.

Under CP30/19, the PRA aims to:

- Complement the policy proposals on operational resilience set out in CP29/19;
- Facilitate greater resilience and adoption of the cloud and other new technologies as set out in the BOE’s response to the ‘Future of Finance’ report;
- Implement the EBA Guidelines. The Draft SS clarifies how the PRA expects banks to approach the EBA Guidelines in the context of its requirements and expectations. In addition, certain chapters in the Draft SS elaborate on the expectations in the EBA Guidelines; and
- Take into account the:
  - EIOPA Guidelines; and
  - EBA’s Guidelines on ICT and security risk management.

### Definitions

CP30/19 relies largely on the definitions set out in the EBA Guidelines. However, the PRA uses the definition of outsourcing from the PRA Rulebook, i.e., an arrangement of any form between a firm and a service provider, whether a supervised entity or not, by which that service provider performs a process, a service or an activity, whether directly or by sub-outsourcing, which would otherwise be undertaken by the firm itself. As under the EBA Guidelines and EIOPA Guidelines, it is for firms to assess whether an arrangement with a third party meets the definition of outsourcing. Firms should assume that any activity, function or service performed by a third party in a prudential context (as defined in the PRA Rulebook) falls within the definition of outsourcing. CP30/19 uses the term “material outsourcing” to mean the same as “critical or important” under the EBA Guidelines.

### Who does it apply to?

This consultation paper is relevant to all UK banks, building societies and PRA-designated investment firms, insurance and reinsurance firms and groups in scope of Solvency II, including the Society of Lloyd’s and managing agents, and third country branches (UK branches of overseas banks and insurers). A limited part of the proposals in CP30/19 are also relevant to credit unions and non-directive firms.

### Timing

At the time of publication of this Paper the PRA’s intention was to publish its final policy on this topic in the second half of 2020, with the policy coming into force shortly thereafter. However, the PRA acknowledged that it will need to provide firms with longer implementation periods for certain requirements; for example, to give them sufficient time to revise all existing outsourcing agreements (as required under the EBA Guidelines and the EIOPA Guidelines).

### Internal governance/overarching requirements

CP30/19 makes clear that existing PRA rules relating to governance, such as Threshold Conditions and SMCR (as defined below), are relevant to outsourcings. Additionally, the PRA sets out in the Draft SS the governance-level rules that it expects firms to comply with. It is apparent from the Draft SS that the PRA has leveraged the fact that the requirements under the EBA Guidelines and the EIOPA Guidelines will already apply to some of the firms, by aligning its own proposals with these requirements. The PRA expects firms complying with the Draft SS to:

- Ensure an appropriate level of board engagement and allocated responsibility;
- Maintain an outsourcing policy and an outsourcing register of all new and legacy outsourcing arrangements (the appendix to the Draft SS adds PRA’s commentary to the EBA Guidelines’ Register described in Part One);
- Undertake thorough vendor due diligence and pre-contractual assessments;
- Review and update all legacy outsourcing arrangements, including to bring them in line with the minimum contractual requirements discussed further below;
- Ensure an appropriate level of protection for outsourced data and systems;
- Have in place sufficient audit arrangements, including to mitigate concentration risks;
- Manage any sub-outsourcing; and
- Develop and implement business continuity plans and exit strategies.

The PRA further notes that some arrangements between firms and third parties which may fall outside the definition of ‘outsourcing’ in the EBA Guidelines may also be relevant to the financial stability of the UK, the PRA’s

statutory objectives, the operational resilience of firms and/or the performance of regulated activities or the BOE's resolution objectives (e.g., the sharing of data with third parties, including through application programming interfaces, and the purchase of third party hardware or software (e.g., 'off the shelf' artificial intelligence/machine learning models)). The PRA highlights that whilst third party arrangements falling outside the definition of 'outsourcing' may not be subject to specific requirements on outsourcing, they are however within the scope of the PRA Principles and general requirements and expectations, particularly on governance, risk management and systems and controls. The Draft SS therefore reminds firms of their obligation to comply with certain PRA rules (e.g., Fundamental Rules 2, 3, 5 and 6, Conduct Rules and Insurance (Conduct Standards and Senior Manager Conduct Rules/Standards Parts)) in relation to all their arrangements with third parties, irrespective of whether they fall under the definition of outsourcing.

### Contractual requirements

Firms are also expected to implement the contractual requirements set out in the Draft SS when formalising outsourcing agreements. The PRA emphasises that all outsourcing arrangements must be in writing and, for all material outsourcing arrangements, the agreement should address data security, audit rights, sub-outsourcing and business continuity and exit plans.

### Application to intra-group/intra-entity arrangements

The PRA's proposals in CP30/19 will apply to any intra-group outsourcing arrangements entered into by firms.

CP30/19 provides that intra-group outsourcing is subject to the same requirements and expectations as outsourcing to service providers outside a firm's group and should not be treated as being inherently less risky. Nonetheless, in case of intra-group outsourcing, firms may in their compliance efforts take into account the level of control and influence they have over the intra-group service provider, in line with the MiFID II Delegated Regulation and Solvency II Delegated Regulation. The PRA suggests that firms may adjust the proportionality of their approach towards meeting the expectations of the Draft SS, and sets out examples of steps that firms can take, including:

- Adjusting their vendor due diligence;
- Relying on their group's stronger negotiating and purchasing power to enter into group-wide arrangements with external parties;
- Adapting certain clauses in outsourcing agreements; or
- Relying on group policies and procedures as long as they comply with their UK legal and regulatory obligations and allow them to manage relevant risks, e.g., group cyber-security or data protection policies.

The PRA also reiterates that third country branches or subsidiaries that outsource to parent companies outside the UK and which are bound by policies, procedures or agreements set by the overseas parent company should ensure that the outsourced service is provided in compliance with UK legal and regulatory requirements. Such firms are also advised by the PRA to implement mechanisms for escalating issues with service providers to the parent company.

The Draft SS further provides that for intra-group outsourcing, firms should consider leveraging their existing compliance with other rules to comply with the Draft SS. For example, the PRA refers to the operational continuity in resolution framework and notes that the provision of services by intra-group service companies, if clearly documented, can facilitate mapping of services to recipient entities and provide greater clarity about which shared services need to continue in resolution. In addition, the PRA notes that, for banks whose intra-group outsourcing arrangements are subject to the requirements in Operational Continuity Chapter 4 and Ring-Fenced Bodies chapters 9 and 12, compliance with these requirements may also mean those banks meet certain expectations in the Draft SS in respect of intra-group outsourcing arrangements (e.g., on business continuity and exit plans).

## BOE, FCA and PRA Shared Operational Resilience Policy

A key objective for the BOE, PRA and FCA is to put in place a stronger regulatory framework to promote the operational resilience of firms and financial market infrastructures. The three consultation papers which constitute the Shared Operational Resilience Policy propose new rules, principles, expectations and guidance to meet such objective. Due to different legislation and regulatory frameworks under which the PRA, the FCA and the BOE operate, the approach taken by each supervisory authority is not identical but their intended outcomes are aligned.

The PRA's consultation paper on operational resilience ("CP29/19"), emphasises that firms' approach to outsourcing is key in achieving operational resilience and consequently names it as one of the five core supporting requirements for its operational resilience policy. Further, the PRA encourages firms to read CP30/19 (discussed above) in conjunction with CP29/19. With the aim of achieving operational resilience, the PRA proposes that firms consider the delivery of important business services against each of the three strategic outcomes outlined below. For each of these we have also highlighted the key outsourcing considerations that should form part of this assessment.

The shared operation resilience policy applies to banks, building societies, PRA designated investment firms, Solvency II firms, Recognised Investment Exchanges, Enhanced scope Senior Managers & Certification Regime firms and entities authorised or registered under the Payment Services Regulations 2017 and/or the Electronic Money Regulations 2011.



## Identifying important business services

The PRA proposes that firms consider the chains of activities which constitute each relevant business service to identify which parts of the chain are critical to delivery, and ensure that such critical parts are operationally resilient. This assessment includes all outsourced services. Should an element of the chain of activities have the potential to disrupt or cause harm to consumers or market integrity, threaten the viability of firms or cause instability in the financial system, it should be deemed a critical service.

## Set impact tolerances

The PRA proposes that firms set impact tolerances for each important business service, including those which are outsourced, which would quantify the maximum level of disruption an important business service would tolerate. The impact tolerances should be set at a point at which disruption to a firm's important business services would pose a risk to either the firm's safety and soundness or financial stability, and should be set as a clear metric (e.g., the maximum duration of an IT service slow-down or blackout).

## Ensuring the firm remains within the impact tolerances

Firms should be able to remain within impact tolerance for important business services, irrespective of whether or not they use third parties in the delivery of these services. With this in mind, the PRA suggests the following methods of ensuring firms remain within their impact tolerances.

- Mapping
- To ensure that an important business service could remain within its impact tolerance, firms need to understand how the service is delivered and how it could be disrupted. This could become quite complex for some firms, especially where the people, processes, technology, facilities and information (resources) used to deliver important business services are outsourced.
- The PRA proposes that firms identify and document the people, processes, technology, facilities and information that support their important business services. Through mapping, firms could highlight vulnerabilities in how important business services are being delivered, and then take action to remediate the vulnerabilities so that important business services remain within their impact tolerances.
- Firms will be expected to develop their own mapping methodology and assumptions to best fit their business. Therefore, a business with a significant reliance on outsourced services would need to adapt their mapping methodology accordingly.
- Scenario testing
- The PRA proposes that firms test their ability to deliver important business services within impact tolerances in severe but plausible scenarios. This would help inform firms of vulnerabilities of internally provided and outsourced services, which might mean they are unable to remain within impact tolerances. Testing would also help firms to consider how they would respond to disruptions when they occur, including their incident management procedures, which would inform them about their ability to remain within impact tolerances. The entire chain of activities that have been identified as the important business service should be considered when developing testing plans.
- Self-assessment
- The PRA proposes requiring firms to document a self-assessment of their compliance with the operational resilience policy. The PRA would expect firms to summarise the vulnerabilities they have identified to the delivery of their important business services, outline the scenario testing performed and the findings from the tests. The PRA would expect firms to indicate what actions are planned to improve their ability to remain within impact tolerances and demonstrate that the timing for the implementation of these is reasonable. In relation to intra-group outsourced important business services, if testing found that such a service could not be delivered within its impact tolerance firms would be expected to work with other members of their group to take action.

## Senior Managers and Certification Regime (“SMCR”)

The SMCR is the individual accountability regime applicable to individuals working in financial services firms. The three key elements of the SMCR are: (i) the Senior Managers Regime, which focuses on individuals performing senior management functions on behalf of a firm, whether physically based in the UK or overseas; (ii) the Certification Regime, which applies to employees who could pose a risk of significant harm to their firm or any of its customers (e.g., staff who give investment advice or administer benchmarks); and (iii) the FCA and PRA Conduct Rules, which are high-level requirements that apply to most individuals working for an authorised firm. For an explanation of which parts of the SMCR are relevant to outsourcing arrangements, please see Schedule 4.

## Dates of entry into force

- In force from 7 March 2016 for UK banks, building societies, credit unions, PRA-designated investment firms, and branches of foreign banks operating in the UK.
- In force from 10 December 2018 for insurers, and branches of foreign insurers operating in the UK.
- In force from 9 December 2019 for all other Financial Services and Markets Act 2000 (“FSMA”) authorised firms, and branches of foreign firms operating in the UK.



## Systems and Controls Rules (“SYSC” Chapter of the FCA Handbook) and the equivalent Parts of the PRA Rulebook (General Organisational Requirements; Outsourcing)

The purpose of SYSC is to: (i) encourage directors and senior managers to take appropriate practical responsibility for their firms’ arrangements on matters likely to be of interest to the FCA; (ii) increase certainty by amplifying Principle 3 of the FCA Principles, under which a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems; (iii) encourage firms to vest responsibility for effective and responsible organisation in specific directors and senior managers; and (iv) create a common platform of organisational and systems and controls requirements for all firms. The SYSC rules and the equivalent PRA Rulebook provisions reflect many of the EU-wide requirements; however, there are additional requirements in place that must also be followed by the relevant firms to whom they apply. For a list of the outsourcing rules and guidance in SYSC, please see Schedule 4.

The SYSC rules outline several notification requirements. Firstly, a firm should notify the FCA when it intends to rely on a third party for the performance of operational functions which are critical or important for performance (SYSC 8.1.12). Secondly, insurers should take particular care to manage material outsourcing arrangements and a firm should notify the FCA when it intends to enter into a material outsourcing arrangement (SYSC 13.9.2).

## Brexit – UK branches of EEA firms and the Temporary Permissions Regime

EEA firms currently operating through a passport in the UK under the existing European passporting framework will require a Part 4A permission under the Financial Services and Markets Act (FSMA) to be able to continue carrying out regulated activities in the UK after the end of the transition period. However, to facilitate a smooth and orderly exit from the EU, HM Treasury has legislated such that a Temporary Permissions Regime (“TPR”) will take effect from the end of the transition period. The aim of the TPR is to avoid a cliff edge by allowing firms to continue carrying out business in the UK for a limited period after the passporting regime ends while they seek authorisation from UK regulators.

Under the TPR, a firm that is authorised to carry on regulated activities in the UK through Freedom of Establishment or Freedom of Services passporting can obtain a deemed Part 4A permission to carry on those activities for a maximum of three years from the end of the transition period. A passporting firm that already has a Top-Up Permission would obtain a deemed variation of that permission.

EEA firms subject to the TPR (including EEA firms that have submitted an application for variation of an existing ‘top-up’ permission) will fall under the UK outsourcing regimes as stated in this section, and the supervision of the UK regulators. However, the principle of ‘substituted compliance’ will apply meaning that if firms can demonstrate they continue to comply with the equivalent home state rules in respect of their UK business (including where this is on a voluntary basis if the relevant rules cease to cover UK business) they will be deemed to comply with the UK rules (for EEA firms that are varying an existing ‘top-up’ permission, substituted compliance will apply to the activities not covered by their existing Part 4A permission). Changes to the relevant competent authority will however take effect from the end of the transition period. Please see the mapping table at the start of this document for further details.

## Enforcement

Both the FCA and the PRA have taken enforcement action against firms for outsourcing-related failings. A number of key cases (and the core learnings from said cases) are highlighted in this section. The highlighted cases show that the UK regulators tend to bring action for failings in relation to the outsourcing of services under the FCA and PRA Principles, in favour of the specific outsourcing guidelines or rules as highlighted within this document. Enforcement to date has been completed at a National Competent Authority (“NCA”) level rather than at a European level, and is consequently subject to divergence in approach between NCAs.

### R. Raphael & Sons plc (2019)

The FCA and PRA each issued separate fines to R. Raphael & Sons plc (“**Raphaels**”), for failing to manage its outsourcing arrangements properly between April 2014 and December 2016. This was the second fine of this kind issued to Raphaels by the PRA (the first is discussed below). The Final Notices were each issued on 29 May 2019, and the fines were for £775,100<sup>16</sup> and £1,121,512,<sup>17</sup> respectively.

The regulators found that Raphaels failed to have adequate processes to enable it to understand and assess the business continuity and disaster recovery arrangements of its outsourced service providers – particularly how they would support the continued operation of its card programmes during a disruptive event. The absence of such processes posed a risk to Raphaels’ operational resilience and exposed its customers to a serious risk of harm. These risks crystallised on 24 December 2015 when a technology incident occurred at a card processor leading to the unavailability of authorisation and processing services for over eight hours.

<sup>16</sup> FCA, 29 May 2019, “Final Notice: R. Raphael & Sons plc”, available at: <<https://www.fca.org.uk/publication/final-notices/r-raphael-sons-plc-final-notice-2019.pdf>>

<sup>17</sup> PRA, 29 May 2019, “Final Notice: R. Raphael & Sons plc”, available at: <<https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/regulatory-action/r-raphael-and-sons-plc-final-notice-may-2019.pdf>>

The joint FCA and PRA investigation identified weaknesses throughout the firm's outsourcing systems and controls, which Raphaels ought to have known about since April 2014. These included a lack of adequate consideration of outsourcing within its board and departmental risk appetites, the absence of processes for identifying critical outsourced services, and flaws in its initial and on-going due diligence of outsourced service providers.<sup>18</sup>

The PRA found that Raphaels had breached PRA Principles 2 (Skill, Care and Diligence), 5 (Risk Management) and 6 (Control), whilst the FCA found that Raphaels breached FCA Principles 2 (Skill, Care, and Diligence) and 3 (Management and Control). These principles require that a firm must: (i) conduct its business with due skill, care and diligence; (ii) take reasonable care to organise and control its affairs responsibly and effectively; and (iii) have adequate risk management systems in place.

This case underlines the importance of establishing proper outsourcing systems and controls, including putting in place contractual documentation that does more than just recite general regulatory requirements, engaging in appropriate initial and ongoing due diligence of service providers, and ensuring appropriate risk identification and management processes. The case also stresses the importance of understanding the business continuity arrangements of service providers, what to expect during a disruptive event, and how communications concerning such events will be managed.

### Liberty Mutual Insurance Europe SE

The FCA published a Final Notice to Liberty Mutual Insurance Europe SE ("LMIE") on 29 October 2018,<sup>19</sup> fining LMIE £5,280,800. LMIE had outsourced the performance of administrative functions associated with mobile phone insurance to a third party, including its claims and complaints handling functions. The FCA found that LMIE breached FCA Principle 3 (Management and Control) and Principle 6 (Customers' Interests) as the company had failed to ensure that it had adequate systems and controls in place to oversee the third party contractor, resulting in poor results for customers.

Specifically, LMIE did not undertake an adequate risk assessment in relation to the outsourcing, nor did it adequately plan for ongoing monitoring of the arrangements. Although the arrangements were overseen by the Compliance Function and the Audit Committee, there was a lack of oversight from the board and senior management, resulting in thousands of customers unfairly being denied cover for their claims.

This case demonstrates the importance of having proper oversight of outsourced service providers' activities, understanding their business model, and addressing concerns at an early stage. The case also emphasises that it is not acceptable for a firm to leave a third party to design such an offering, without the firm having adequate systems and controls in place to ensure that the third party's activities comply with the relevant regulatory requirements.

### R. Raphael & Sons plc (2015)

The PRA's first Final Notice<sup>20</sup> to Raphaels was published in November 2015. Raphaels was fined £1,278,165 for failing to manage its outsourcing arrangements in respect of the provision of ATMs across the UK. The PRA found that Raphaels had breached Principle 3 (Management and Control) of the PRA Principles.

Raphaels had entered into a joint venture with a company in its group for the provision of ATMs. The group company performed activities such as the payment of third parties on its behalf and the replenishment of the ATMs. The PRA found that in relation to these activities, Raphaels failed to enter into a written agreement until 2010, 21 months after the provision of services had begun. As a result, Raphaels had inadequate systems and controls, meaning that funds were transferred from its bank accounts by a team subcontracted by a service provider without the knowledge or consent of Raphaels. This resulted in Raphaels providing inaccurate and misleading capital and liquidity reports to the PRA. The PRA found that Raphaels failed in a number of areas including failure to:

- Carry out suitable due diligence in respect of its outsourcing;
  - Manage the risks associated with the outsourcing, or to oversee important operational functions. The written agreement that was entered into after the service provision began was, according to the PRA, "materially deficient in setting out the rights and obligations of the respective parties";
  - Specify in the written agreement appropriate arrangements for Raphaels' oversight of the outsourced functions; and
  - Ensure proper supervision of the group company performing the outsourced finance function.
- This case highlights the importance of completing proper diligence on service providers both prior to entering outsourcing arrangements with them, and on an ongoing basis thereafter. The case also emphasises that intra-group arrangements should be treated with the same diligence as third party arrangements, and that such arrangements should always be properly documented.

<sup>18</sup> FCA, 30 May 2019, "FCA and PRA jointly fine Raphaels Bank £1.89m for outsourcing failings", available at: <<https://www.fca.org.uk/news/press-releases/fca-and-pra-jointly-fine-raphaels-bank-1-89-million-outsourcing-failings>>

<sup>19</sup> FCA, 29 October 2018, "Final Notice: Liberty Mutual Insurance Europe SE", available at: <<https://www.fca.org.uk/publication/final-notice/liberty-mutual-insurance-europe-se-2018.pdf>>

<sup>20</sup> PRA, 27 November 2015, "PRA fines Raphaels Bank £1,278,165 for outsourcing failures", available at: <<https://www.bankofengland.co.uk/news/2015/november/pr-fines-raphaels-bank-for-outsourcing-failures>>

## Stonebridge International Insurance Ltd

Stonebridge International Insurance Ltd (“**Stonebridge**”) was fined £8,373,600 in August 2014<sup>21</sup> for breaching Principle 3 (Management and Control) and Principle 6 (Customers’ Interests) of the FCA Principles between April 2011 and December 2012. Stonebridge had outsourced its sales and customer service operations for certain insurance products to third party intermediaries. Amongst other things, the FCA found that Stonebridge had:

- Designed telesales scripts for its outsourcing firms that did not provide clear, fair and balanced information;
- Put in place poor systems and controls, and inadequate oversight in relation to outsourcing the sales and cancellation process;
- Failed to ensure that its board and executive committee oversaw the outsourced service providers effectively;
- Failed to implement adequate systems and controls before customer services were outsourced to new providers; and
- Failed to resource its compliance department adequately to enable it to establish and monitor systems and controls at the intermediaries to an adequate standard.

This enforcement action provides an example of the importance not only of implementing outsourcing oversight functions, but also of ensuring that relevant functions are compliant with regulation prior to being outsourced. Almost inevitably, the outsourcing of a non-compliant service, without proper oversight, will result in future regulatory issues.

## UK Parliamentary Inquiries

### Treasury Committee inquiry into TSB service disruption incident

The Treasury Committee launched an inquiry to investigate the service disruption incident that occurred at TSB in April 2018. The incident arose from TSB’s efforts to migrate its computer systems to a new platform using outsourced service providers, which resulted in amongst other things: (i) incorrect balances being shown to customers; (ii) access issues; and (iii) customers being given access to other customers’ accounts. The Treasury Committee considered TSB’s preparation for, implementation of, and results of the systems migration, and TSB’s handling of the problems that ensued. The inquiry was closed on 5 November 2019 following the dissolution of Parliament for the 2019 General Election. Prior to Parliament’s closure, a number of interested parties, including the FCA CEO, Andrew Bailey provided evidence to the inquiry.<sup>22</sup>

The Treasury Committee’s interest in this incident highlights the level of scrutiny that may be placed on a firm as a result of an outsourcing infringement, and provides another example of the importance of due diligence on outsourced services providers and continued oversight.

### IT failures in the financial services sector inquiry

The Treasury Committee launched an inquiry in November 2018 to investigate the common causes of operational incidents within the financial services sector, the effects of such incidents on consumers, and whether the regulators have the relevant skills to adequately hold people to account. The inquiry was launched in response to a series of IT failures at banks and other financial institutions, including Equifax, TSB, Visa, Barclays, Cashplus and The RBS. The Treasury Committee acknowledged that against a back-drop of branch closures and customers increasingly being ushered to use online services, millions of customers have been affected by the uncertainty and disruption caused by failures of banking IT systems. Within this changing landscape the availability of reliable online services is vital. The inquiry was closed on 5 November 2019 following the dissolution of Parliament for the 2019 General Election.

This inquiry shows that Parliament acknowledges the changing face of the financial services industry and is interested in protecting consumers from the effects of negligent outsourcing. Further, it shows that Parliament has an appetite to scrutinise regulators and the financial services industry for their shortcomings in outsourcing, particularly in IT services.

## Banking Secrecy Rules


Banking secrecy rules may apply in the context of an outsourcing arrangement involving bank customers’ information. Banking secrecy is an agreement by banks to keep client information confidential. The ethos behind such laws is to protect clients’ privacy and to provide an attractive place in order for clients to keep their financial activities anonymous. There is no single European-level legal framework governing banking secrecy rules.

Banking secrecy rules can prove difficult to comply with, given a bank’s need to disclose information in its day-to-day activities such as providing routine services to clients, making inter-company transfers or outsourcing some services to third party providers. The obligations on banks, and if applicable, their officers and employees, vary across jurisdictions. However, laws are not limited to national banks – established branches of foreign banks can also be caught under the remit of national banking secrecy laws. Banks in contravention of the banking secrecy rules may be subject to fines, regulatory action, private lawsuits, and sometimes criminal sanctions.

---

<sup>21</sup> FCA, 7 August 2014, “Final Notice to Stonebridge International Insurance Limited”, available at: <<https://www.fca.org.uk/publication/final-notice/stonebridge-international-insurance-limited.pdf>>.

<sup>22</sup> UK Parliament, “Service Disruption at TSB inquiry” available at: <<https://www.parliament.uk/business/committees/committees-a-z/commons-select/treasury-committee/inquiries/parliament-2017/tsb-sabadell-17-19/>> (accessed: 01/11/2019).



Despite Europe's lack of a single legal framework regulating banking secrecy, national obligations exist. In England, in *Tournier v. National Provincial and Union Bank of England*<sup>23</sup> it was held that this duty is implied on bankers except where applicable law requires disclosure, a duty to the public to disclose exists, the interests of the bank require disclosure, or the customer gives consent (which can be implied). Though an English Court of Appeal decision, the *Tournier* case has weight in many common law jurisdictions that have cited it (e.g., Ireland). However, it should be noted that the secrecy principle may conflict with increasing political demands for tax transparency, as exemplified by rules such as Council Directive 2011/16/EU (often referred to as DAC 6), which contains mandatory reporting requirements for disclosure of cross-border arrangements.

---

<sup>23</sup> [1923] 12 WLUK 61

# SCHEDULE 1

## TEMPLATE OUTSOURCING REGISTER

Outsourcing arrangement	
[Enter, as you prefer, a number or name for a specific outsourcing arrangement]	
Outsourcing entity	
Name of outsourcing entity	[Insert]
Corporate registration number	[Insert]
Legal entity identifier	[Insert]
Registered address	[Insert]
Name of parent company (if any)	[Insert]
Service provider	
Name of the service provider	[Insert]
Corporate registration number	[Insert]
Legal entity identifier (where available)	[Insert]
Registered address and contact details	[Insert]
Name of parent company (if any)	[Insert]
General	
Reference number	[Insert]
Start date	[Insert]
Renewal date	[Insert]
End date	[Insert]
Notice periods	[Insert]
Current status	[Insert]
Description	
Brief description of the outsourced function	[Insert]
Details on the data outsourced	[Insert]
Process or transfer of personal data to the service provider (Yes/No)	[Insert]
Category of function (e.g., IT, control)	[Insert]



Location	
Country or countries from where the service is performed	[Insert]
Country or countries to which the service is performed	[Insert]
Country or region where the data is located	[Insert]
Criticality of importance	
Whether or not the outsourced function is considered critical or important (Yes/No)	[Insert]
If Yes, a brief summary of the reasons why the outsourced function is considered critical or important	[Insert]
Cloud outsourcing	
Is this a cloud outsourcing? Only if Yes should the other yellow columns be completed.	[Insert]
Cloud service and deployment models (i.e., public/private/hybrid/community)	[Insert]
Specific nature of the data to be held	[Insert]
Countries or regions where the data will be stored	[Insert]
Review date	
Date of the most recent assessment of the criticality or importance of the outsourced function	[Insert]
Institutional protection schemes	
List of the institutions, payment institutions and other firms within the scope of the prudential consolidation or institutional protection scheme, where applicable, that make use of the outsourcing	[Insert]
Whether the service provider or sub-service provider is part of the group or a member of the institutional protection scheme or owned by institutions or payment institutions within the group or owned by members of an institutional protection scheme (Yes/No)	[Insert]
Risk assessment	
Date of the most recent risk assessment	[Insert]
A brief summary of the main results of the most recent risk assessment	[Insert]
Decision making	
The individual or decision-making body (e.g., the management body) that approved the outsourcing arrangement	[Insert]

<b>Governing law</b>	
The governing law of the outsourcing agreement	[Insert]
<b>Audits</b>	
Date of the most recent audit (where applicable)	[Insert]
Date of the next scheduled audit (where applicable)	[Insert]
<b>Sub-contractor (where applicable, i.e., material parts of a critical or important function are sub-outsourced)</b>	
Name of the sub-contractor(s)	[Insert]
Country/countries where the sub-contractor(s) are registered	[Insert]
Country/countries where the service will be performed	[Insert]
If applicable, country or region where the data will be stored	[Insert]
<b>Alternatives</b>	
Outcome of the assessment of the service provider's substitutability (Easy / Difficult / Impossible)	[Insert]
Possibility of reintegrating a critical or important function into the institution or the payment institution	[Insert]
Impact of discontinuing the critical or important function	[Insert]
Identification of alternative service providers in line with columns AF-AH	[Insert]
<b>Time-criticality</b>	
Whether the outsourced critical or important function supports business operations that are time-critical (Yes/No)	[Insert]
<b>Cost</b>	
Estimated annual budget cost	[Insert]

# SCHEDULE 2

## PART A – CHECKLIST FOR CONTRACTUAL REQUIREMENTS UNDER THE EBA GUIDELINES

	Guideline Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
<b>Section 13 – General Contract Requirements</b>				
1.	Para 74	The rights and obligations of the institution, the payment institution and the service provider should be clearly allocated and set out in a written agreement.	<p><b><i>It generally goes without saying that any outsourcing agreement should be in writing and that it should clearly allocate each party's rights and responsibilities:</i></b></p> <ul style="list-style-type: none"> <li>• Ensure the agreement is in writing, signed, and is as clear as possible regarding the scope of services. The agreement should include, for example, detailed service descriptions identifying the specific services and deliverables being provided by the service provider, along with any relevant performance standards (stating to what level of performance each service will be provided).</li> <li>• The agreement should also contain any customer dependencies that underpin such supplier services (which are carefully drafted as a closed list of clear obligations with specific, limited consequences if missed).</li> <li>• “Joint” obligations/deliverables should be avoided wherever possible; instead focus on what each party will provide.</li> </ul>	
2.	Para 75	<b>The outsourcing agreement for critical or important functions should set out at least:</b>	<p><b><i>The following Paragraph 75 requirements are stated to be a minimum and therefore entities need to consider, based on the nature of the outsourcing, whether stronger or additional controls are appropriate (e.g., where an outsourcing is particularly critical or risky).</i></b></p> <p><b><i>Paragraph 75 presumes that the outsourced function is critical or important as defined under the EBA Guidelines. Such an assessment should be made at the outset to determine whether and to what extent the EBA Guidelines apply. If it is unclear, we would recommend erring on the side of caution by meeting these requirements:</i></b></p> <ul style="list-style-type: none"> <li>• Where the outsourcing is critical or important, ensure that the agreement meets all of the requirements of Paragraph 75 identified below:</li> </ul>	
3.	Para 75 (a)	A clear description of the outsourced function to be provided.	<p><b><i>The outsourcing contract must contain a thorough description of the outsourced function; the more detailed the service description, the better for both parties.</i></b></p> <ul style="list-style-type: none"> <li>• Include clearly drafted recitals that explain the nature and purpose of the relevant outsourcing; this can provide useful context when interpreting the service descriptions.</li> </ul>	

Guideline Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
		<ul style="list-style-type: none"> <li>• Include detailed service descriptions (often in a separate schedule), identifying the specific services and deliverables to be provided by the service provider, along with any relevant timescales and performance standards (stating to what level of performance each service will be provided).</li> <li>• Include a closed list of “customer dependencies” that underpin service provider’s services (which are carefully drafted as a closed list of clear, specific, measurable obligations with specific, limited consequences if missed).</li> </ul>	
4.	Para 75 (b) The start date and end date, where applicable, of the agreement and the notice periods for the service provider and the institution or payment institution.	<p><b><i>A start date should always be included and should distinguish between the effective date of the agreement and the commencement date of the relevant services (i.e., when the agreement must come into operation vs when the specific services must come into operation), if different. It is common practice to include an end date and any termination rights for each party. Notice periods are required and may be a point of negotiation. In an outsourcing context, the notice period should in particular account for the time it may take to replace the necessary arrangements for the outsourced function.</i></b></p> <ul style="list-style-type: none"> <li>• Include clearly drafted “Term” and “Termination” clauses in the agreement. These should set out, as a minimum: <ul style="list-style-type: none"> <li>○ The effective date of the agreement - i.e., when it becomes binding on both parties – this is often but not always (i.e., where the agreement needs to apply retrospectively) linked to the signing date.</li> <li>○ The commencement date for each of the relevant services (noting they may be different for different services). This may be linked to the completion of a transition period / transition plan.</li> <li>○ The date at which the agreement will terminate, unless renewed in accordance with its terms.</li> <li>○ Any rights for either party to extend the term of the agreement, including any minimum notice periods (e.g., “the Customer may extend this agreement by a further one year period on the same terms and conditions by providing no less than four weeks’ written notice to Supplier prior to the expiry of the then-current term”).</li> <li>○ Any rights for either party to terminate the agreement, including any minimum notice periods prior to such termination being deemed effective.</li> </ul> </li> </ul>	
5.	Para 75 (c) The governing law of the agreement.	<p><b><i>While the EBA Guidelines do not specify the requirement for a jurisdiction/ADR clause, we would typically expect to see both included in any outsourcing contract. Parties are advised to:</i></b></p>	

Guideline Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
		<ul style="list-style-type: none"> <li>• Include a governing law clause.</li> <li>• Include a clearly drafted jurisdiction/alternative dispute resolution (ADR) clause.</li> </ul>	
6.	Para 75 (d) The parties' financial obligations.	<p><b>While parties' financial obligations are invariably included in all outsourcing agreements, where they are critical or important, it is even more important that they are clear from the face of the agreement and do not leave room for dispute. Parties are advised to:</b></p> <ul style="list-style-type: none"> <li>• Include a charges / fees schedule that clearly sets out the charging basis and the specific charges for each of the services being provided. The schedule should include details on: <ul style="list-style-type: none"> <li>○ How the charges are calculated (e.g., time and materials, fixed, consumption based, etc.). Relevant pricing books / rate cards should be included.</li> <li>○ The extent to which inflation / CPI / currency fluctuations will be applied.</li> <li>○ In what circumstances the charges can/cannot be reopened by either party (e.g., a change in scope or other price sensitive change).</li> <li>○ When and how the supplier can invoice for the charges.</li> <li>○ When and how the customer should pay the invoices.</li> <li>○ How overpayments are refunded to the customer.</li> <li>○ How invoicing/payment disputes are resolved by the parties.</li> <li>○ Each parties' rights of set-off.</li> <li>○ Whether and how interest is payable on late payments.</li> <li>○ Which party is responsible for relevant taxes.</li> </ul> </li> </ul>	
7.	Para 75 (e) Whether the sub-outsourcing of a critical or important function, or material parts thereof, is permitted and, if so, the conditions specified in Section 13.1 that the sub-outsourcing is subject to.  [See also rows 20 to 33.]	<p><b>An outsourcing agreement for critical or important functions needs to be clear on whether the subcontracting of any/all of the obligations/services of the service provider are permitted, and if so in what circumstances and subject to what restrictions.</b></p> <p>[See also rows 20 to 33.]</p>	
8.	Para 75 (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, including the possible storage location, and the conditions to be met, including a requirement to notify the institution or payment institution if the service provider	<p><b>An outsourcing agreement will typically state expressly where the services are being provided from (and to). However, the EBA Guidelines additionally clarify that the location of data must be specified. The final EBA Guidelines now also helpfully clarify that, in general, it will be sufficient to specify the region or country of the data (as opposed to the specific location) unless the institution, payment institution or competent authority requires more detailed information to be</b></p>	



Guideline Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
	proposes to change the location(s).	<p><b><i>provided, e.g., to prepare an audit. Parties are advised to:</i></b></p> <ul style="list-style-type: none"> <li>• Include a description of the service locations – being the regions or countries where the function is provided from. Many outsourcing agreements (particularly those involving infrastructure services) will specify the precise address of the locations (e.g., data centre location, call centre location, etc.).</li> <li>• Include a description of any service recipient locations – being the regions or countries to which services are provided (e.g., where service recipients will be located).</li> <li>• Include information about the regions or countries where data will be kept and processed (if applicable). A map of the relevant data flows may be useful for this purpose.</li> <li>• Include any conditions, including notice or consent requirements by service provider if there is a proposed change of location(s). We note that it is typical (though not required by the EBA Guidelines) to include any notice/consent requirements where the customer wants to change any service location.</li> </ul>	
9.	Para 75 (g)  Where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as specified in Section 13.2.  [See also rows 34 to 37].	<ul style="list-style-type: none"> <li>• Include data provisions, if applicable, specified below in Section 13.2 (<u>Security of data and systems</u>).</li> </ul> <p>[See also rows 34 to 37].</p>	
10.	Para 75 (h)  The right of the institution or payment institution to monitor the service provider's performance on an ongoing basis.	<p><b><i>This is a standard requirement in an outsourcing contract. Negotiation points tend to surround the type, extent and frequency of the monitoring.</i></b></p> <ul style="list-style-type: none"> <li>• Include the right to monitor service provider's performance.</li> </ul>	
11.	Para 75 (i)  The agreed service levels, which should include precise quantitative and qualitative performance targets for the outsourced function to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met.	<p><b><i>Effective outsourcing agreements require service levels, and the targets must be tailored to the parties' requirements.</i></b></p> <ul style="list-style-type: none"> <li>• Include service levels with quantitative and qualitative performance targets.</li> </ul>	
12.	Para 75 (j)  The reporting obligations of the service provider to the institution or payment institution, including the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the critical or important function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements and, as appropriate, the obligations to submit reports of the internal	<p><b><i>It is standard for outsourcing agreements to contain notification obligations but this requirement clarifies that service recipients may press for far-reaching communication obligations (e.g., any developments that <u>may</u> have a material impact on the service provider's <u>ability to effectively carry out the function</u>).</i></b></p> <ul style="list-style-type: none"> <li>• Include an obligation on the service provider to report potentially material developments and, as appropriate, submit internal audit reports.</li> </ul>	

Guideline Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
	audit function of the service provider.		
13.	Para 75 (k) Whether the service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested.	<b>While it is not a requirement under the EBA Guidelines, insurance is market practice and minimises risk for all parties.</b> <ul style="list-style-type: none"> <li>Specify whether service provider's insurance is required / not required.</li> </ul>	
14.	Para 75 (l) The requirements to implement and test business contingency plans.	<b>It is highly recommended for parties to an outsourcing to consider business contingency plans. It appears from this requirement that both parties must include in the agreement requirements to implement and test their respective business contingency plans.</b> <ul style="list-style-type: none"> <li>Include provisions regarding business contingency plans.</li> </ul>	
15.	Para 75 (m) Provisions that ensure that the data that is owned by the institution or payment institution can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider.	<b>While outsourcing agreements normally provide for these situations, this requirement should serve as a reminder for parties to include (i) sufficient IP and data ownership provisions and (ii) provisions detailing how to retain access to the data if the service provider becomes insolvent or similar.</b> <ul style="list-style-type: none"> <li>Include accommodation for continued access to data, in case of service provider's insolvency, resolution or discontinuation.</li> </ul>	
16.	Para 75 (n) The obligation of the service provider to cooperate with the competent authorities and resolution authorities of the institution or payment institution, including other persons appointed by them.	<b>Outsourcing arrangements involving heavily regulated institution or payment institutions subject to the EBA Guidelines would normally provide, to varying degrees, for this requirement.</b> <ul style="list-style-type: none"> <li>Include an obligation on the service provider to cooperate with competent authorities.</li> </ul>	
17.	Para 75 (o) For institutions, a clear reference to the national resolution authority's powers, especially to Articles 68 and 71 of Directive 2014/59/EU ("BRRD"), and in particular a description of the 'substantive obligations' of the contract in the sense of Article 68 of BRRD.	<b>Due to this requirement, institutions will become contractually obliged to align their exit strategies in relation to the outsourcing arrangement with that required under the Bank Recovery and Resolution Directive.</b> <ul style="list-style-type: none"> <li>Include specific references to Articles 68 and 71 of BRRD.</li> </ul>	
18.	Para 75 (p) The unrestricted right of institutions, payment institutions and competent authorities to inspect and audit the service provider with regard to, in particular, the critical or important outsourced function, as specified in Section 13.3.  [See also rows 38 to 62.]	<ul style="list-style-type: none"> <li>Include inspection and audit rights, specified below in Section 13.3 (<a href="#">Access, information and audit rights</a>).</li> </ul> <p>[See also rows 38 to 62.]</p>	
19.	Para 75 (q) Termination rights, as specified in Section 13.4.  [See also rows 63 to 72.]	<ul style="list-style-type: none"> <li>Include termination rights, specified below in Section 13.4 (<a href="#">Termination rights</a>).</li> </ul> <p>[See also rows 63 to 72.]</p>	

Guideline Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
<b>Section 13.1 – Sub-outsourcing of critical or important functions</b>			
20.	Para 76	The outsourcing agreement should specify whether or not sub-outsourcing of critical or important functions, or material parts thereof, is permitted.	<p><b><i>An outsourcing agreement for critical or important functions needs to be clear on whether the subcontracting of any/all of the obligations/services of the service provider are permitted, and if so in what circumstances and subject to what restrictions.</i></b></p> <ul style="list-style-type: none"> <li>• Include a clearly drafted subcontracting clause that either permits or prohibits the onward subcontracting of the service provider's obligations/services to a third party. This should make clear which elements of the services can/cannot be subcontracted (e.g., the clause may include various materiality thresholds by reference to the criticality/risk of the service being outsourced, below which subcontracting is permitted without additional consent).</li> <li>• Where subcontracting is permitted, the subcontracting clause must address the conditions specified below (see rows 21 to 33).</li> </ul>
21.	Para 77	If sub-outsourcing of critical or important functions is permitted, institutions and payment institutions should determine whether the part of the function to be sub-outsourced is, as such, critical or important (i.e., a material part of the critical or important function) and, if so, record it in the register.	<p><b><i>The EBA Guidelines prescribe in Section 11 that all institutions subject to the EBA Guidelines must maintain a register of all their outsourcing arrangements. This is a new requirement that was not included in the EBA Guidelines' predecessor. For assistance, please see the Latham &amp; Watkins template at Schedule 1.</i></b></p> <ul style="list-style-type: none"> <li>• If sub-outsourcing a material part of a critical or important function, list it accordingly in the register.</li> </ul>
22.	Para 78	<b>If sub-outsourcing is permitted, the written agreement should:</b>	<ul style="list-style-type: none"> <li>• Where sub-outsourcing is permitted, ensure that the agreement meets all of the requirements of para 78 identified below:</li> </ul>
23.	Para 78 (a)	Specify any types of activities that are excluded from sub-outsourcing.	<p><b><i>Per good practice, parties should consider what types of activities they would be comfortable with being sub-outsourced, keeping in mind the overarching accountability requirements under the EBA Guidelines and other regulations.</i></b></p> <ul style="list-style-type: none"> <li>• Specify all excluded activities.</li> </ul>
24.	Para 78 (b)	Specify the conditions to be complied with in the case of sub-outsourcing.	<p><b><i>To the extent that sub-outsourcing is permitted, parties should include any conditions, for the purpose of risk exposure and complying with the specific items in this paragraph 78.</i></b></p> <ul style="list-style-type: none"> <li>• Include conditions for sub-outsourcing.</li> </ul>
25.	Para 78 (c)	Specify that the service provider is obliged to oversee those services that it has subcontracted to ensure that all contractual obligations between the service provider and the institution or payment institution are continuously met.	<p><b><i>It should be given that the sub-outsourcing terms or activities should not conflict with the terms of the outsourcing agreement. This requirement also imposes a de facto monitoring obligation on the service provider vis-à-vis the sub-outsourcing entity.</i></b></p> <ul style="list-style-type: none"> <li>• Include an obligation on the service provider to oversee sub-outsourced services in light of the outsourcing agreement's terms.</li> </ul>

	Guideline Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
26.	Para 78 (d)	Require the service provider to obtain prior specific or general written authorisation from the institution or payment institution before sub-outsourcing data.	<p><b>Sub-outsourcing of data, for example, where the service provider uses cloud services, is easily overlooked in negotiations as it may not relate directly to the outsourced function. However privacy laws and this requirement under the EBA Guidelines highlight the importance of addressing such sub-outsourcing by requiring prior authorisation.</b></p> <ul style="list-style-type: none"> <li>• Include a provision which requires prior authorisation for sub-outsourcing of data.</li> </ul>	
27.	Para 78 (e)	Include an obligation of the service provider to inform the institution or payment institution of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. This includes planned significant changes of subcontractors and to the notification period; in particular, the notification period to be set should allow the outsourcing institution or payment institution at least to carry out a risk assessment of the proposed changes and to object to changes before the planned sub-outsourcing, or material changes thereof, come into effect.	<p><b>It is customary to include in the outsourcing agreement a notification obligation for these types of changes. It is notable that this requirement expressly requires the notification period, normally a point of negotiation, to be long enough for risk assessment and objection. This may favour the institutions or payment institutions.</b></p> <ul style="list-style-type: none"> <li>• Include an obligation on the service provider to inform of any planned sub-outsourcing or material changes.</li> <li>• Ensure any related notification period in the agreement is long enough to allow for risk assessment and objection by the institution or payment institution.</li> </ul>	
28.	Para 78 (f)	Ensure, where appropriate, that the institution or payment institution has the right to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required.	<p><b>This right for the institution or payment institution to object or consent would normally be considered in discussions around sub-outsourcing. It should be noted that the EBA Guidelines do not impose an absolute right, as they specify where appropriate.</b></p> <ul style="list-style-type: none"> <li>• Include right for institution or payment institution to object or explicitly consent to intended sub-outsourcing, where appropriate.</li> </ul>	
29.	Para 78 (g)	Ensure that the institution or payment institution has the contractual right to terminate the agreement in the case of undue sub-outsourcing, e.g., where the sub-outsourcing materially increases the risks for the institution or payment institution, or where the service provider sub-outsources without notifying the institution or payment institution.	<p><b>This requirement prescribes a termination right for the institution or payment institution that is not always included in outsourcing agreements. While it may be met with resistance in negotiations, the language of the EBA Guidelines is clear on this point.</b></p> <ul style="list-style-type: none"> <li>• Include right for institution or payment institution to terminate in case of undue sub-outsourcing.</li> </ul>	
30.	Para 79	<b>Institutions and payment institutions should agree to sub-outsourcing only if the subcontractor undertakes to:</b>	<ul style="list-style-type: none"> <li>• Where sub-outsourcing is permitted, ensure that the agreement meets all of the requirements of para 79 identified below:</li> </ul>	
31.	Para 79 (a)	Comply with all applicable laws, regulatory requirements and contractual obligations.	<p><b>Any sub-contractor to an outsourcing agreement would be expected to undertake these obligations.</b></p> <ul style="list-style-type: none"> <li>• Include an obligation on the sub-contractor to comply with applicable laws, regulatory requirements and contractual obligations.</li> </ul>	

	Guideline Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
32.	Para 79 (b)	Grant the institution, payment institution and competent authority the same contractual rights of access and audit as those granted by the service provider.	<p><b>Normally service providers and sub-contractors may not expect such extensive access and audit rights. The EBA Guidelines strictly require such rights in order to allow the sub-outsourcing.</b></p> <ul style="list-style-type: none"> <li>• Include right for institution, payment and competent authority to access and audit the sub-contractor.</li> </ul>	
33.	Para 80	Institutions and payment institutions should ensure that the service provider appropriately oversees the sub-service providers, in line with the policy defined by the institution or payment institution. If the sub-outsourcing proposed could have material adverse effects on the outsourcing arrangement of a critical or important function or would lead to a material increase of risk, including where the conditions in paragraph 79 would not be met, the institution or payment institution should exercise its right to object to the sub-outsourcing, if such a right was agreed, and/or terminate the contract.	<p><b>These requirements are sometimes expected in an outsourcing arrangement.</b></p> <p><b>The requirement may be addressed by including the relevant policies into the service provider's obligation under para 78 (c).</b></p> <p><b>The second requirement illustrates the importance of negotiating a right for the institution or payment institution to object (in line with para 78 (f)), as this requirement may otherwise force the institution or payment institution to terminate if the service provider proposes sub-outsourcing to a sub-contractor which could materially increase risk.</b></p> <ul style="list-style-type: none"> <li>• Include an obligation on the service provider to oversee sub-contractor according to institution or payment institution's policies.</li> <li>• If sub-outsourcing could have material adverse effects on the outsourcing arrangement or lead to a material increase of risk, include an obligation on the institution or payment institution to object (if possible) or terminate.</li> </ul>	
<b>Section 13.2 – Security of data and systems</b>				
34.	Para 81	Institutions and payment institutions should ensure that service providers, where relevant, comply with appropriate IT security standards.	<p><b>Addressing IT security standards has become increasingly important and common since the introduction of privacy laws such as the GDPR. Provided this requirement is <u>relevant</u>, parties may include an appropriate contractual obligation on the service provider.</b></p> <ul style="list-style-type: none"> <li>• Where relevant, include an obligation on the service provider to comply with IT security standards.</li> </ul>	
35.	Para 82	Where relevant (e.g., in the context of cloud or other ICT outsourcing), institutions and payment institutions should define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis.	<p><b>As above, this is important in light of privacy laws such as the GDPR and are therefore increasingly common in outsourcing agreements. Institutions and payment institutions should take particular note of the need to, and be prepared to, monitor compliance on an ongoing basis. The EBA Guidelines do not impose an absolute obligation here, as they specify <u>where relevant</u>.</b></p> <ul style="list-style-type: none"> <li>• Where relevant, include defined data and system security requirements and monitor compliance.</li> </ul>	
36.	Para 83	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 and payment institutions should adopt a risk-	<p><b>Institutions and payment institutions approach to data and information security is reflected in outsourcing agreements to varying degrees. This particular requirement, which focuses on outsourcing involving personal or confidential data, does not specify how parties should reflect the risk-based approach in the</b></p>	



Guideline Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
	based approach to data storage and data processing location(s) (i.e., country or region) and information security considerations.	<p><b>outsourcing agreement. Following applicable GDPR requirements, such as incorporating standard Model Clauses for any data transfers, would likely demonstrate a risk-based approach.</b></p> <ul style="list-style-type: none"> <li>Ensure that the provisions of the agreement reflect a risk-based approach to data storage and processing location(s) (i.e., country or region) and information security.</li> </ul>	
37.	Para 84	<p>Without prejudice to the requirements under GDPR, institutions and payment institutions, when outsourcing (in particular to third countries), should take into account differences in national provisions regarding the protection of data. Institutions and payment institutions should ensure that the outsourcing agreement includes the obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to the institution or payment institution (e.g., the protection of personal data and that banking secrecy or similar legal confidentiality duties with respect to clients' information, where applicable, are observed).</p>	<p><b>As above and as expressly mentioned in the EBA Guidelines, parties are expected to prepare the outsourcing agreement and the arrangement in line with the GDPR.</b></p> <ul style="list-style-type: none"> <li>Ensure that the data protection provisions of the agreement account for differences in national data protection laws.</li> <li>Include an obligation on the service provider to protect confidential, personal or otherwise sensitive information and comply with all legal requirements.</li> </ul>
<b>Section 13.3 – Access, information and audit rights</b>			
38.	Para 85	<p>Institutions and payment institutions should ensure within the written outsourcing arrangement that the internal audit function is able to review the outsourced function using a risk-based approach.</p>	<p><b>The right to audit the service provider is common practice in outsourcing agreements. This requirement highlights that such rights need to be sufficiently flexible to accommodate any increased risk.</b></p> <ul style="list-style-type: none"> <li>Include a provision to ensure that the internal audit function can review the outsourced function.</li> </ul>
39.	Para 86	<p>Regardless of the criticality or importance of the outsourced function, the written outsourcing arrangements between institutions and service providers should refer to the information gathering and investigatory powers of competent authorities and resolution authorities under Article 63(1)(a) of BRRD and Article 65(3) of CRD IV with regard to service providers located in a Member State and should also ensure those rights with regard to service providers located in third countries.</p>	<p><b>The parties should ensure that the outsourcing agreement contains a provision to this effect.</b></p> <ul style="list-style-type: none"> <li>The agreement refers to the information gathering and investigatory powers of competent authorities and resolution authorities under Article 63(1)(a) of BRRD and Article 65(3) of CRD IV.</li> </ul>
40.	Para 87	<p><b>With regard to the outsourcing of critical or important functions, institutions and payment institutions should ensure within the written outsourcing agreement that the</b></p>	<p><b>We note this is an exhaustive list, not a minimum.</b></p> <ul style="list-style-type: none"> <li>Ensure that the agreement meets all of the requirements of para 87 identified below:</li> </ul>

	Guideline Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
		service provider grants them and their competent authorities, including resolution authorities, and any other person appointed by them or the competent authorities, the following:		
41.	Para 87 (a)	Full access to all relevant business premises (e.g., head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors ('access and information rights').	<p><b><i>The extent and frequency of access and information rights tend to be heavily negotiated in outsourcing agreements. This requirement means that service providers will have to accept far-reaching rights of this type.</i></b></p> <ul style="list-style-type: none"> <li>• Ensure in the agreement the service provider grants full access and information rights.</li> </ul>	
42.	Para 87 (b)	Unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.	<p><b><i>Similar to the requirement for access and information rights; whereas normally audit rights are negotiated, this requirement effectively guarantees that service providers have to allow unrestricted auditing to show compliance with both regulatory and contractual requirements.</i></b></p> <ul style="list-style-type: none"> <li>• Ensure in the agreement the service provider grants unrestricted audit rights.</li> </ul>	
43.	Para 88	For the outsourcing of functions that are not critical or important, institutions and payment institutions should ensure the access and audit rights as set out in paragraph 87 (a) and (b) and Section 13.3, on a risk-based approach, considering the nature of the outsourced function and the related operational and reputational risks, its scalability, the potential impact on the continuous performance of its activities and the contractual period. Institutions and payment institutions should take into account that functions may become critical or important over time.	<p><b><i>The EBA Guidelines set out the approach that would normally be expected in negotiations of access and audit rights, i.e., that they should be tailored to the risk of the arrangement. Since this provision does not prescribe specific rights or rights, it mostly serves as guidance in respect of the factors that should be considered in negotiations.</i></b></p> <ul style="list-style-type: none"> <li>• For non-critical or important outsourcing, ensure in the agreement that the service provider grants rights in line with those required under paragraphs 87 (a) and (b) and this Section 13.3, adjusted for risk.</li> </ul>	
44.	Para 89	Institutions and payment institutions should ensure that the outsourcing agreement or any other contractual arrangement does not impede or limit the effective exercise of the access and audit rights by the institutions and payment institutions, competent authorities or third parties appointed by them to exercise these rights.	<p><b><i>This requirement reiterates the importance and priority which the parties must give to the access and audit rights. To meet this requirement, the drafting in the outsourcing agreement and any related contractual agreements should state that potentially conflicting provisions are without prejudice to the access and audit rights.</i></b></p> <ul style="list-style-type: none"> <li>• Ensure in the agreement access and audit rights are not impeded by the outsourcing agreement or any other contractual arrangement.</li> </ul>	
45.	Para 90	Institutions and payment institutions should exercise their access and audit rights, determine the audit frequency and areas to be audited on a risk-based approach and adhere to relevant, commonly accepted,	<p><b><i>It is standard for access and audit rights in well-drafted outsourcing contracts to provide for these requirements.</i></b></p> <ul style="list-style-type: none"> <li>• Ensure in the agreement that access and audit rights are based on a risk-based</li> </ul>	

	Guideline Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
		national and international audit standards.	approach and national and international audit standards.	
46.	Para 91	<b>Without prejudice to their final responsibility regarding outsourcing arrangements, institutions and payment institutions may use:</b>	<ul style="list-style-type: none"> <li>Depending on the nature of the agreement and the negotiations between the parties, and provided the institutions and payment institutions' responsibility is not affected, include any of the relevant provisions of para 91 identified below:</li> </ul>	
47.	Para 91 (a)	Pooled audits organised jointly with other clients of the same service provider, and performed by them and these clients or by a third party appointed by them, to use audit resources more efficiently and to decrease the organisational burden on both the clients and the service provider.	<ul style="list-style-type: none"> <li>Include pooled audits with other clients of the same service provider.</li> </ul>	
48.	Para 91 (b)	Third-party certifications and third-party or internal audit reports, made available by the service provider.	<ul style="list-style-type: none"> <li>Include third-party certifications.</li> <li>Include third-party or internal audit reports.</li> </ul>	
49.	Para 92	For the outsourcing of critical or important functions, institutions and payment institutions should assess whether third-party certifications and reports as referred to in paragraph 91(b) are adequate and sufficient to comply with their regulatory obligations and should not rely solely on these reports over time.	<ul style="list-style-type: none"> <li>Include certifications and reports that are sufficient for the institutions and payment institutions' regulatory obligations.</li> <li>Ensure in the agreement that certifications and reports are not solely relied on.</li> </ul>	
50.	Para 93	<b>Institutions and payment institutions should make use of the method referred to in paragraph 91(b) only if they:</b>	<ul style="list-style-type: none"> <li>Where using the certifications and reports described in para 91(b), all the requirements of para 93 identified below:</li> </ul>	
51.	Para 93 (a)	Are satisfied with the audit plan for the outsourced function.	<p><b><i>As is usually the case in outsourcing agreements, the parties should consider the specific form of any audit plan and specify any appropriate conditions. Parties should include provisions to that effect to ensure that the audit plans are consistently satisfactory to the institutions and payment institutions as required by the EBA Guidelines.</i></b></p> <ul style="list-style-type: none"> <li>Include clear requirements for a satisfactory audit plan.</li> </ul>	
52.	Para 93 (b)	Ensure that the scope of the certification or audit report covers the systems (i.e., processes, applications, infrastructure, data centres, etc.) and key controls identified by the institution or payment institution and the compliance with relevant regulatory requirements.	<p><b><i>The institutions and payment institutions should include these requirements as required conditions for any certification or audit report.</i></b></p> <ul style="list-style-type: none"> <li>Ensure the certifications or reports in the agreement cover all relevant systems, key controls and regulatory requirements.</li> </ul>	
53.	Para 93 (c)	Thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify	<p><b><i>This requirement is in line with the obligation on the institutions and payment institutions to maintain responsibility as mentioned in para 91 and as expected in an outsourcing agreement.</i></b></p>	

	Guideline Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
		that the reports or certifications are not obsolete.	<p><b>Importantly this requirement may limit the institutions and payment institutions' ability to agree to full reliance on the certifications or reports in the outsourcing agreement.</b></p> <ul style="list-style-type: none"> <li>• Include an assessment mechanism for content and status of certifications or audits.</li> </ul>	
54.	Para 93 (d)	Ensure that key systems and controls are covered in future versions of the certification or audit report.	<p><b>In line with the above requirements, the parties may ensure compliance by specifying this as conditions in the outsourcing agreement.</b></p> <ul style="list-style-type: none"> <li>• Ensure in the agreement that future reports include key systems and controls.</li> </ul>	
55.	Para 93 (e)	Are satisfied with the aptitude of the certifying or auditing party (e.g., with regard to rotation of the certifying or auditing company, qualifications, expertise, performance/verification of the evidence in the underlying audit file).	<p><b>In line with the above requirements, the parties may ensure compliance by specifying this as conditions in the outsourcing agreement.</b></p> <ul style="list-style-type: none"> <li>• Include clear requirements for satisfactory aptitude of certifying or auditing third party.</li> </ul>	
56.	Para 93 (f)	Are satisfied that the certifications are issued and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place.	<p><b>In line with the above requirements, the parties may ensure compliance by specifying this as conditions in the outsourcing agreement.</b></p> <ul style="list-style-type: none"> <li>• Include clear requirements to ensure certificates or audits meet recognised professional standards and include a test of the key controls.</li> </ul>	
57.	Para 93 (g)	Have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective.	<p><b>In line with the above requirements, the parties may ensure compliance by specifying this as conditions in the outsourcing agreement.</b></p> <ul style="list-style-type: none"> <li>• Include reasonable right for institution or payment institution to request an expanded scope of the certifications or reports.</li> </ul>	
58.	Para 93 (h)	Retain the contractual right to perform individual audits at their discretion with regard to the outsourcing of critical or important functions.	<p><b>It is expected in an outsourcing agreement to retain some right to perform an audit in place of a certification or other third party mechanism but the circumstances of when such a right would be triggered may be negotiated. This requirement under the EBA Guidelines clarifies that the audit should be at the institution or payment institution's discretion. This must therefore be reflected in the drafting of the outsourcing agreement.</b></p> <ul style="list-style-type: none"> <li>• Include right for institution or payment institution to perform audit at discretion.</li> </ul>	
59.	Para 94	In line with the EBA Guidelines on ICT risk assessment under the SREP, institutions should, where relevant, 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. Taking into account Title I, payment institutions should also have internal ICT control mechanisms,	<p><b>Outsourcing parties tend to extensively discuss whether security penetration testing should be allowed and, if so, the form it should take. On this point, the EBA Guidelines do not impose an absolute requirement, as the provision states <u>where relevant</u>.</b></p> <ul style="list-style-type: none"> <li>• Where relevant, ensure the agreement allows for security penetration testing.</li> </ul>	



Guideline Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
	including ICT security control and mitigation measures.	<ul style="list-style-type: none"> <li>Where relevant, ensure the agreement is consistent with the EBA Guidelines on ICT risk assessment under the SREP.</li> </ul>	
60.	Para 95	Before a planned on-site visit, institutions, payment institutions, competent authorities and auditors or third parties acting on behalf of the institution, payment institution, or competent authorities should provide reasonable notice to the service provider, unless this is not possible due to an emergency or crisis situation or doing so would lead to a situation where the audit would no longer be effective.	<p><b><i>This requirement conforms with the provisions normally seen in outsourcing agreements.</i></b></p> <ul style="list-style-type: none"> <li>Include requirement for reasonable notice prior to on-site visit, unless emergency.</li> </ul>
61.	Para 96	When performing audits in multi-client environments, care should be taken to ensure that risks to another client's environment (e.g., impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated.	<ul style="list-style-type: none"> <li>For audits in multi-client environment, ensure the agreement provides that necessary care must be taken in respect of other clients.</li> </ul>
62.	Para 97	Where the outsourcing arrangement carries a high level of technical complexity, for instance in the case of cloud outsourcing, the institution or payment institution should verify that whoever is performing the audit – whether it is its internal auditors, the pool of auditors or external auditors acting on its behalf – has appropriate and relevant skills and knowledge to perform relevant audits and/or assessments effectively. The same applies to any staff of the institution or payment institution reviewing third-party certifications or audits carried out by service providers.	<p><b><i>Outsourcing agreements normally contain a provision to this effect. This requirement should therefore be a guiding point for drafting such provisions.</i></b></p> <ul style="list-style-type: none"> <li>Where there is a high level of technical complexity, include clear requirements to ensure person performing the audit has appropriate skills and knowledge.</li> </ul>
<b>Section 13.4 – Termination rights</b>			
63.	Para 98	<b>The outsourcing arrangement should expressly allow the possibility for the institution or payment institution to terminate the arrangement, in accordance with applicable law, including in the following situations:</b>	<p><b><i>We note these requirements are stated to be a minimum.</i></b></p> <ul style="list-style-type: none"> <li>Ensure that the agreement meets, in express terms, all the requirements of para 98 identified below:</li> </ul>
64.	Para 98 (a)	Where the provider of the outsourced functions is in a breach of applicable law, regulations or contractual provisions.	<p><b><i>This requirement is standard practice in outsourcing agreements.</i></b></p> <ul style="list-style-type: none"> <li>Include right for institution or payment institution to terminate for breach.</li> </ul>
65.	Para 98 (b)	Where impediments capable of altering the performance of the outsourced function are identified.	<p><b><i>This requirement provides a broad termination right which would normally involve extensive negotiations. It appears to go beyond what a standard force majeure clause would include</i></b></p>



	Guideline Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
			<p><i>by referring to impediments <u>capable of altering the performance</u>. Outsourcing agreements must provide for this requirement but the specific form of it is likely to be negotiated.</i></p> <ul style="list-style-type: none"> <li>• Include right for institution or payment institution to terminate for potential impediment.</li> </ul>	
66.	Para 98 (c)	Where there are material changes affecting the outsourcing arrangement or the service provider (e.g., sub-outsourcing or changes of sub-contractors).	<p><i>This requirement similarly provides a broad termination right but is aimed at changes <u>affecting the arrangement and is therefore more common and acceptable in practice.</u></i></p> <ul style="list-style-type: none"> <li>• Include right for institution or payment institution to terminate for material changes.</li> </ul>	
67.	Para 98 (d)	Where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information.	<ul style="list-style-type: none"> <li>• Include right for institution or payment institution to terminate for weaknesses in data management.</li> </ul>	
68.	Para 98 (e)	Where instructions are given by the institution's or payment institution's competent authority, e.g., in the case that the competent authority is, as a result of the outsourcing arrangement, no longer in a position to effectively supervise the institution or payment institution.	<p><i>In outsourcing arrangements in heavily regulated industries such as that subject to the EBA Guidelines, it is common and necessary to include a termination right due to regulatory action. The requirement still allows flexibility for drafting and negotiation, e.g., as to the nature of the instructions by the competent authority.</i></p> <ul style="list-style-type: none"> <li>• Include right for institution or payment institution to terminate in case of instructions by competent authority.</li> </ul>	
69.	Para 99	<b>The outsourcing arrangement should facilitate the transfer of the outsourced function to another service provider or its re-incorporation into the institution or payment institution. To this end, the written outsourcing arrangement should:</b>	<p><i>We note these requirements are stated to be a minimum.</i></p> <ul style="list-style-type: none"> <li>• Ensure that the agreement meets all the requirements of para 99 identified below:</li> </ul>	
70.	Para 99 (a)	Clearly set out the obligations of the existing service provider, in the case of a transfer of the outsourced function to another service provider or back to the institution or payment institution, including the treatment of data.	<p><i>We would expect outsourcing agreements to account for potential transfers between service providers or back to the institution or payment institution. The requirement to also account for data is in line with other requirements under the EBA Guidelines and the GDPR.</i></p> <ul style="list-style-type: none"> <li>• Include clear obligations of the existing service provider in case of a transfer, including regarding data.</li> </ul>	
71.	Para 99 (b)	Set an appropriate transition period, during which the service provider, after the termination of the outsourcing arrangement, would continue to provide the outsourced function to reduce the risk of disruptions.	<p><i>It is common for outsourcing agreements to include transitional arrangements in line with this requirement.</i></p> <ul style="list-style-type: none"> <li>• Include appropriate transition period and arrangements in case of a transfer.</li> </ul>	

	Guideline Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
72.	Para 99 (c)	Include an obligation of the service provider to support the institution or payment institution in the orderly transfer of the function in the event of the termination of the outsourcing agreement.	<p><i>As above, it is common for outsourcing agreements to include transitional arrangements in line with this requirement.</i></p> <ul style="list-style-type: none"> <li>• Include an obligation on the service provider to support with transfer in case of termination.</li> </ul>	

# SCHEDULE 2

## PART B - CHECKLIST FOR CONTRACTUAL REQUIREMENTS UNDER THE CLOUD RECOMMENDATIONS

### Key definitions

- “**cloud services**” means 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;
- “**public cloud**” means cloud infrastructure available for open use by the general public;
- “**private cloud**” means cloud infrastructure available for the exclusive use by a single institution;
- “**community cloud**” means cloud infrastructure available for the exclusive use by a specific community of institutions, including several institutions of a single group; and
- “**hybrid cloud**” means cloud infrastructure that is composed of two or more distinct cloud infrastructures.

	Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
<b>Section 4.1 – Materiality assessment</b>				
1.	Para 4.1.1	Outsourcing institutions should, prior to any outsourcing of their activities, assess which activities should be considered as material.	<p><b><i>The materiality assessment will be important to assess the significance of the outsourcing to the institution. If the outsourcing is of a critical business function, then this assessment will help to determine the contingency plans to put in place should the cloud service provider fail or deteriorate to an unacceptable degree. The main risks (including the risk of data loss) will be identified, which will help to prepare contingency plans to mitigate any potential losses.</i></b></p> <p>Institutions should perform this assessment of activities’ materiality and for outsourcing to cloud service providers in particular, taking into account all of the following:</p> <ul style="list-style-type: none"> <li>• The criticality and inherent risk profile of the activities to be outsourced, i.e., whether the activities are critical to the business continuity/viability of the institution and its obligations to customers.</li> <li>• The direct operational impact of outages, and related legal and reputational risks.</li> <li>• The impact that any disruption of the activity might have on the institution’s revenue prospects.</li> <li>• The potential impact that a confidentiality breach or failure of data integrity could have on the institution and its customers.</li> </ul>	

Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
<b>Section 4.2 – Duty to adequately inform supervisors</b>			
2.	Para 4.2.2	<p>Outsourcing institutions should adequately inform the competent authorities of material activities to be outsourced to cloud service providers.</p>	<p><b><i>The outsourcing institution will have to make the above information available to regulators, this is a new requirement. Authorities and regulators may ask for additional information about risk analysis, exit options and internal audits.</i></b></p> <p>Institutions should make available to the competent authorities the following information:</p> <ul style="list-style-type: none"> <li>• The name of the cloud service provider and the name of its parent company (if any);</li> <li>• A description of the activities and data to be outsourced;</li> <li>• The country or countries where the service is to be performed (including the location of data);</li> <li>• The service commencement date;</li> <li>• The last contract renewal date (where applicable);</li> <li>• The applicable law governing the contract; and</li> <li>• The service expiry date or next contract renewal date (where applicable).</li> </ul>
3.	Para 4.2.3	<p>Risk analysis whereby the competent authority may ask for additional information for the material activities to be outsourced.</p>	<p><b><i>The regulators may ask for additional information on exit options and contingency planning to ensure the outsourcing institution has plans in place in the event the cloud service provider does not fulfil the contractual expectations. This may help to offset risks as plans are considered. It is important to ensure that diligence has been documented and an “audit trail” has been created to document the company’s compliance.</i></b></p> <p>The additional information on risk analysis may include:</p> <ul style="list-style-type: none"> <li>• Whether the cloud service provider has a business continuity plan that is suitable for the services provided to the outsourcing institution;</li> <li>• Whether the outsourcing institution has an exit strategy in case of termination by either party or disruption of the provision of services by the cloud service provider; and</li> </ul>

Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
			<ul style="list-style-type: none"> <li>Whether the outsourcing institution maintains the skills and resources necessary to adequately monitor the outsourced activities.</li> </ul>
4.	Para 4.2.4	<p>The outsourcing institution should maintain an updated register of information on all its material and non-material activities outsourced to cloud service providers at the institution and group level.</p>	<p><b><i>These requirements should also be documented in the contract with the cloud service provider to allow for disclosure of information to regulators upon request to demonstrate compliance with maintaining registers as well as providing the copy of the agreement freely if required.</i></b></p> <p><b><i>The outsourcing institution should:</i></b></p> <ul style="list-style-type: none"> <li>Maintain an up-to-date register of information on all material and non-material activities outsourced to cloud service providers at the institution and group level.</li> <li>Make available to the competent authority a copy of the outsourcing agreement and related information recorded in that register upon request, irrespective of whether the activity outsourced to a cloud service provider has been assessed by the institution as material.</li> </ul>
5.	Para 4.2.5	<p>The register of information on material and non-material activities should contain certain information as detailed in the columns to the right.</p>	<p><b><i>These requirements are new and place stricter requirements on outsourcing institutions. Outsourcing institutions will need to ensure that the information contained in the register is accurate and up to date.</i></b></p> <p>The following information should be included in the register:</p> <ul style="list-style-type: none"> <li>The name of the cloud service provider and the name of its parent company (if any);</li> <li>A description of the activities and data to be outsourced;</li> <li>The country or countries where the service is to be performed (including the location of data);</li> <li>The service commencement date;</li> <li>The last contract renewal date (where applicable);</li> </ul>



Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
		<ul style="list-style-type: none"> <li>• The applicable law governing the contract;</li> <li>• The service expiry date or next contract renewal date (where applicable);</li> <li>• The type of outsourcing (the cloud service model and cloud deployment model, i.e., public/ private/ hybrid/ community cloud);</li> <li>• The parties receiving cloud services under the outsourcing agreement;</li> <li>• Evidence of the approval for outsourcing by the management body or its delegated committees, if applicable;</li> <li>• The names of any subcontractors if applicable;</li> <li>• The country where the cloud service provider/main subcontractor is registered;</li> <li>• Whether the outsourcing has been assessed as material (yes/no);</li> <li>• The date of the institution's last materiality assessment of the outsourced activities;</li> <li>• Whether the cloud service provider/subcontractor(s) supports business operations that are time critical (yes/no);</li> <li>• An assessment of the cloud service provider's substitutability (as easy, difficult or impossible);</li> <li>• Identification of an alternate service provider, where possible; and</li> <li>• The date of the last risk assessment of the outsourcing or subcontracting arrangement.</li> </ul>	
<b>Section 4.3 – Access and audit rights</b>			
6.	Paras 4.3.6, 4.3.7, 4.3.8 and 4.3.9	For the purposes of cloud outsourcing, outsourcing institutions should ensure that they have in place an agreement in writing with the cloud service provider whereby the latter undertakes the obligation to provide the institution with a right of access and a right of audit.	<b><i>The Recommendations have allowed for the use of pooled audits which is a new addition. This makes the process flexible and provides outsourcing institutions with further options. The decision of whether to use a third party auditor or a pooled audit will be a commercial decision and will differ from institution to institution.</i></b>

Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
			<p>To meet this requirement, the institution should ensure that the following conditions are agreed in writing with the cloud service provider:</p> <ul style="list-style-type: none"> <li>• To provide to the institution, to any third party appointed for that purpose by the institution and to the institution's statutory auditor full access to its business premises (head offices and operations centres), including the full range of devices, systems, networks and data used for providing the services outsourced (right of access).</li> <li>• To confer to the institution, to any third party appointed for that purpose by the institution and to the institution's statutory auditor, unrestricted rights of inspection and auditing related to the outsourced services (right of audit).</li> </ul> <p>The outsourcing institution should exercise its rights to audit and access in a risk-based manner. Where an outsourcing institution does not employ its own audit resources, it should consider using at least one of the following tools:</p> <ol style="list-style-type: none"> <li>i. Pooled audits organised jointly with other clients of the same cloud service provider, and performed by these clients or by a third party appointed by them, in order to use audit resources more efficiently and to decrease the organisational burden on both the clients and the cloud service provider.</li> <li>ii. Third-party certifications and third-party or internal audit reports made available by the cloud service provider.</li> </ol>
<b>Section 4.4 – Access Rights</b>			
7.	Para 4.4.14	For the right of access, the agreement should contain certain provisions which allow for reasonable time periods to be given and include provisions for cooperation.	<p><b><i>These terms are expected to be included in commercial contracts as they provide for certainty for access and set standards for the cloud service provider.</i></b></p> <p>The following provisions should be included:</p> <ul style="list-style-type: none"> <li>• The party intending to exercise its right of access (institution, competent authority, auditor or third party acting for the institution or the competent</li> </ul>



Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
			<p>authority) should first provide notice in a reasonable time period of the onsite visit to a relevant business premise, unless an early prior notification is not possible due to an emergency or crisis situation.</p> <ul style="list-style-type: none"><li data-bbox="815 443 1225 600">• The cloud service provider is required to fully cooperate with the appropriate competent authorities, as well as the institution and its auditor, in connection with the onsite visit.</li></ul>

	Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
<b>Section 4.5 – Security of data and systems</b>				
8.	Para 4.5.16	<p>The institution prior to outsourcing will need to amongst other things detailed in the column to the right, perform a risk based assessment, decide on appropriate levels of data confidentiality, and consider the use of encryption technologies. These security aspects should be monitored on an on-going basis.</p>	<p><b><i>Understanding the risks of cloud outsourcing is helpful for contingency planning and may mitigate risks in the long term. Key data confidentiality protection provisions can be added into the contract to ensure the terms are followed strictly. Liability can also be apportioned with the inclusion of clauses used to determine risk and responsibility.</i></b></p> <p>Prior to outsourcing and for the purpose of informing the relevant decision, the institution should take the following steps:</p> <ul style="list-style-type: none"> <li>• Identify and classify its activities, processes and related data and systems as to the sensitivity and required protections.</li> <li>• Conduct a thorough risk-based selection of the activities, processes and related data and systems which are under consideration to be outsourced to a cloud computing solution.</li> <li>• Define and decide on an appropriate level of protection of data confidentiality.</li> <li>• Consider the continuity of activities outsourced, and integrity and traceability of data and systems in the context of the intended cloud outsourcing. Institutions should also consider specific measures where necessary for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture.</li> </ul>	
<b>Section 4.7 – Chain outsourcing</b>				
9.	Paras 4.7.21, 4.7.22 and 4.7.23	<p>Institutions should take account of the risks associated with 'chain' outsourcing, where the outsourcing service provider subcontracts elements of the service to other providers.</p> <p>The outsourcing institution should agree to chain outsourcing only if the subcontractor will also fully comply with the obligations</p>	<p><b><i>Institutions should include the provisions listed above in the contract to ensure that service disruptions are kept to a minimum if the cloud service provider uses 'chain' outsourcing, and also to apportion liability should this have an adverse effect. It will be important to allocate risk and ensure these terms are negotiated to suit the needs of the business.</i></b></p>	

Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
	existing between the outsourcing institution and the outsourcing service provider.	<ul style="list-style-type: none"> <li>The outsourcing agreement between the outsourcing institution and the cloud service provider should specify any types of activities that are excluded from potential subcontracting and indicate that the cloud service provider retains full responsibility for and oversight of those services that it has subcontracted.</li> <li>The outsourcing agreement should include an obligation for the cloud service provider to inform the outsourcing institution of any planned significant changes to the subcontractors or the subcontracted services named in the initial agreement that might affect the ability of the service provider to meet its responsibilities.</li> <li>The notification period for those changes should be contractually pre-agreed to allow the outsourcing institution to carry out a risk assessment of the effects of the proposed changes before the actual change in the subcontractors or the subcontracted services comes into effect.</li> <li>In case a cloud service provider plans changes to a subcontractor or subcontracted services that would have an adverse effect on the risk assessment of the agreed services, the outsourcing institution should have the right to terminate the contract.</li> </ul>	

**Section 4.8 – Contingency plans and exit strategies**

10.	Paras 4.8.26, 4.8.27 and 4.8.28	The outsourcing institution should plan and implement arrangements to maintain the continuity of its business in the event that the provision of services by an outsourcing service provider fails or deteriorates to an unacceptable degree. These arrangements should include contingency planning and a clearly defined exit strategy.	<p><b><i>Each agreement needs to be considered in its own context, and the terms above should be negotiated to suit the business, especially the notice periods needed for terminating the cloud outsourcing arrangements. While the terms will be specific on the cloud service provided, the outsourcing institution should try to retain the flexibility to terminate in the event the services are not as agreed.</i></b></p> <ul style="list-style-type: none"> <li>The outsourcing contract should include a termination and exit management clause that allows the</li> </ul>
-----	---------------------------------	---	--



Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
			<p>activities being provided by the outsourcing service provider to be transferred to another outsourcing service provider or to be reincorporated into the outsourcing institution.</p> <p>An outsourcing institution should also ensure that it is able to exit cloud outsourcing arrangements, if necessary, without undue disruption to its provision of services or adverse effects on its compliance with the regulatory regime and without detriment to the continuity and quality of its provision of services to clients. To achieve this, an outsourcing institution should:</p> <ul style="list-style-type: none"> <li>• Develop and implement exit plans that are comprehensive, documented and sufficiently tested where appropriate.</li> <li>• Identify alternative solutions and develop transition plans to enable it to remove and transfer existing activities and data from the cloud service provider to these solutions in a controlled and sufficiently tested manner, taking into account data location issues and maintenance of business continuity during the transition phase.</li> <li>• Ensure that the outsourcing agreement includes an obligation on the cloud service provider to sufficiently support the outsourcing institution in the orderly transfer of the activity to another service provider or to the direct management of the outsourcing institution in the event of the termination of the outsourcing agreement.</li> </ul>

# SCHEDULE 3

## CHECKLIST FOR CONTRACTUAL REQUIREMENTS UNDER THE EIOPA GUIDELINES

Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
<b>Guideline 5 – Documentation requirements</b>			
1.	Paras 23	As part of its governance and risk management system, the undertaking should keep a record of its cloud outsourcing arrangements, for example, in the form of a dedicated register kept updated over time. The undertaking should also maintain a record of terminated cloud outsourcing arrangements for an appropriate retention period.	<p><b><i>These requirements should also be documented in the contract with the cloud service provider to allow for disclosure of information to regulators upon request to demonstrate compliance with maintaining records as well as freely providing the copy of the agreement if required.</i></b></p> <ul style="list-style-type: none"> <li>Recording and updating over time all information on cloud outsourcing arrangements.</li> <li>On request, the outsourcing undertaking should make available to the supervisory authority a copy of the outsourcing agreement and related information recorded, irrespective of whether or not the function outsourced to a cloud service provider has been assessed by the undertaking as a critical or important function.</li> </ul>
2.	Paras 24-25	In case of outsourcing of critical or important operational functions or activities, the undertaking should record all of the information detailed in the column to the right.	<p><b><i>Outsourcing undertakings will need to be mindful that the information recorded is accurate and up to date, and that the below list is stated to be a minimum.</i></b></p> <p>The following information should be recorded:</p> <ul style="list-style-type: none"> <li>The information that the undertaking is required to provide to the supervisory authority, set out under the 'Internal governance/overarching requirements' heading in the EIOPA Guidelines section of Part One;</li> <li>In case of groups, the insurance or reinsurance undertakings and other undertakings within the scope of the prudential consolidation that make use of the cloud services;</li> <li>The date and a summary of the most recent risk assessment of the outsourcing or subcontracting arrangement;</li> </ul>

	Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
			<ul style="list-style-type: none"> <li>Name of the individual or decision-making body that approved the outsourcing;</li> <li>The dates of the most recent and next scheduled audits;</li> <li>If applicable, the names of any subcontractors to which material parts of a critical or important operational function or activity are sub-outsourced, their country of registration, location where they will provide services (including the location of data);</li> <li>An outcome of the assessment of the cloud service provider's substitutability (e.g., easy, difficult or impossible);</li> <li>Whether the outsourced critical or important function or activity supports business operations that are time critical (yes/no);</li> <li>The estimated annual budget costs; and</li> <li>Whether the undertaking has an exit strategy in case of termination by either party or disruption of services by the cloud service provider (yes/no).</li> </ul>	
<b>Guideline 10 – Contractual requirements</b>				
3.	Para 36	The rights and obligations of the undertaking and the cloud service provider should be clearly allocated and set out in a written agreement.	<p><b><i>It generally goes without saying that any outsourcing agreement should be in writing and that it clearly allocates each party's rights and responsibilities:</i></b></p> <ul style="list-style-type: none"> <li>Ensure the agreement is in writing, signed, and is as clear as possible regarding the scope of services. The agreement should include, for example, detailed service descriptions identifying the specific services and deliverables being provided by the cloud service provider, along with any relevant performance standards (stating to what level of performance each service will be provided).</li> <li>The agreement should also contain any customer dependencies that underpin such supplier services (which are carefully drafted as a closed list of clear obligations with specific, limited consequences if missed).</li> </ul>	

	Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
			<ul style="list-style-type: none"> <li>“Joint” obligations/deliverables should be avoided wherever possible; instead focus on what each party will provide.</li> </ul>	
4.	Para 37	<p>Without prejudice to the requirements defined in Article 274 of the Delegated Regulation, in case of outsourcing of critical or important operational functions or activities to a cloud service provider, the written agreement between the undertaking and the cloud service provider should set out:</p>	<p><i>The following Paragraph 37 requirements should be considered a minimum and therefore entities need to consider, based on the nature of the outsourcing, whether stronger or additional controls are appropriate (e.g., where an outsourcing is particularly critical or risky).</i></p> <p><i>Paragraph 37 presumes that the outsourced function is a critical or important operational function as defined under the EIOPA Guidelines. Such an assessment should be made at the outset to determine whether and to what extent the EIOPA Guidelines apply. If it is unclear, we would recommend erring on the side of caution by meeting these requirements:</i></p> <ul style="list-style-type: none"> <li>Ensure that the agreement complies with the requirements under Article 274 of the Solvency II Delegated Regulation.</li> <li>Where the outsourcing is material, ensure that the agreement meets all of the requirements of para 37 identified below:</li> </ul>	
5.	Para 37 (a)	<p>A clear description of the outsourced function to be provided (cloud services, including the type of support services).</p>	<p><i>The outsourcing contract must contain a thorough description of the cloud services; the more detailed the service description, the better for both parties.</i></p> <ul style="list-style-type: none"> <li>Include clearly drafted recitals that explain the nature and purpose of the relevant outsourcing; this can provide useful context when interpreting the service descriptions.</li> <li>Include detailed service descriptions (often in a separate schedule), identifying the specific services and deliverables to be provided by the cloud service provider, along with any relevant timescales and performance standards (stating to what level of performance each service will be provided).</li> <li>Include a closed list of “customer dependencies” that underpin cloud service provider’s services (which are carefully drafted as a closed list of clear, specific, measurable obligations with specific, limited consequences if missed).</li> </ul>	

	Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
6.	Para 37 (b)	The start date and end date, where applicable, of the agreement and the notice periods for the cloud service provider and for the undertaking.	<p><b><i>A start date should always be included and should distinguish between the effective date of the agreement and the commencement date of the relevant services (i.e., when the agreement itself vs when the specific services must come into operation), if different. It is common practice to include an end date and any termination rights for each party. Notice periods are required and may be a point of negotiation. In an outsourcing context, the notice period should in particular account for the time it may take to replace the necessary arrangements for the outsourced function:</i></b></p> <ul style="list-style-type: none"> <li>• Include clearly drafted “Term” and “Termination” clauses in the agreement. These should set out, as a minimum: <ul style="list-style-type: none"> <li>○ The effective date of the agreement – i.e., when it becomes binding on both parties – this is often but not always (i.e., where it needs to apply retrospectively) linked to the signing date.</li> <li>○ The commencement date for each of the relevant Services (noting they may be different for different Services). This may be linked to the completion of a transition period / transition plan.</li> <li>○ The date at which the agreement will terminate, unless renewed in accordance with its terms.</li> <li>○ The date at which, and/or how the agreement will renew or how the parties may renew it.</li> <li>○ Any rights for either party to extend the term of the agreement, including any minimum notice periods (e.g., “the Customer may extend this agreement by a further one year period on the same terms and conditions by providing no less than four weeks’ written notice to Supplier prior to the expiry of the then-current term”).</li> <li>○ Any rights for either party to terminate the agreement, including any minimum notice periods prior to such termination being deemed effective.</li> </ul> </li> </ul>	



	Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
7.	Para 37 (c)	The court jurisdiction and governing law of the agreement.	<p><b><i>We would typically expect to see both governing law and jurisdiction provisions included in any outsourcing contract.</i></b></p> <ul style="list-style-type: none"> <li>• Include a governing law clause.</li> <li>• Include a clearly drafted jurisdiction/alternative dispute resolution (ADR) clause.</li> </ul>	
8.	Para 37 (d)	The parties' financial obligations.	<p><b><i>While parties' financial obligations are invariably included in all outsourcing agreements, where they are arrangements for the outsourcing of critical or important functions, it is even more important that they are clear from the face of the agreement and do not leave room for dispute.</i></b></p> <ul style="list-style-type: none"> <li>• Include a charges / fees schedule which clearly sets out the charging basis and the specific charges for each of the services being provided. These should include details on: <ul style="list-style-type: none"> <li>○ How the charges are calculated (e.g., time, fixed, consumption based, etc.). Relevant pricing books / rate cards should be included.</li> <li>○ The extent to which inflation / CPI / currency fluctuations will be applied.</li> <li>○ In what circumstances the charges can/cannot be reopened by either party (e.g., a change in scope or other price sensitive change).</li> <li>○ When and how the supplier can invoice for the charges.</li> <li>○ When and how the customer should pay the invoices.</li> <li>○ How overpayments are refunded to the customer.</li> <li>○ How invoicing/payment disputes are resolved by the parties.</li> <li>○ Each parties' rights of set-off.</li> <li>○ Whether and how interest is payable on late payments.</li> <li>○ Which party is/are responsible for relevant taxes.</li> </ul> </li> </ul>	
9.	Para 37 (e)	Whether the sub-outsourcing of a critical or important function or activity (or material parts thereof) is permitted, and, if so, the conditions	<p><b><i>An outsourcing agreement needs to be clear on whether the sub-outsourcing of critical or important functions or activities of any/all of the obligations/services of the cloud service</i></b></p>	

	Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
		<p>to which the significant sub-outsourcing is subject.</p> <p>[See also rows 53 to 58.]</p>	<p><b><i>provider are permitted, and if so in what circumstances and subject to what restrictions.</i></b></p> <p>[See also rows 53 to 58.]</p>	
10.	Para 37 (f)	<p>The location(s) (i.e., regions or countries) where relevant data will be stored and processed (location of data centres), and the conditions to be met, including a requirement to notify the undertaking if the cloud service provider proposes to change the location(s).</p>	<p><b><i>It is typical for an outsourcing agreement to state expressly where the services are being provided from (and to). However, the EIOPA Guidelines additionally clarify that the location of data must be specified and that in general, it will be sufficient to specify the region or country of the data (as opposed to the specific location) unless more detailed information must be provided, e.g., to prepare an audit.</i></b></p> <ul style="list-style-type: none"> <li>• Include a description of the service locations – being the regions or countries from where the function is provided. Many outsourcing agreements (particularly those involving infrastructure services) will specify the precise address of the locations (e.g., data centre location, call centre location, etc.).</li> <li>• Include a description of any service recipient locations – being the regions or countries to which services are provided (e.g., where service recipients will be located).</li> <li>• Include information about the regions or countries where data will be kept and processed (if applicable). A map of the relevant data flows may be useful for this purpose.</li> <li>• Include any conditions, including notice or consent requirements by cloud service provider if there is a proposed change of location(s). We note that it is typical (though not required by the EIOPA Guidelines) to include any notice/consent requirements where the customer wants to change any service location.</li> </ul>	
11.	Para 37 (g)	<p>Provisions regarding the accessibility, availability, integrity, confidentiality, privacy and safety of relevant data, taking into account the specifications of Guideline 12.</p> <p>[See also rows 35 to 46].</p>	<ul style="list-style-type: none"> <li>• Include data provisions, if applicable, specified below in Guideline 12 (<a href="#">Security of data and systems</a>).</li> </ul> <p>[See also rows 35 to 46].</p>	
12.	Para 37 (h)	<p>The right of the undertaking to monitor the cloud service</p>	<p><b><i>This is a standard requirement in an outsourcing contract. Negotiation points tend</i></b></p>	

Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes	
	provider's performance on a regular basis.	<p><b>to surround the type, extent and frequency of the monitoring.</b></p> <ul style="list-style-type: none"> <li>Include the right to monitor cloud service provider's performance.</li> </ul>		
13.	Para 37 (i)	<p>The agreed service levels, which should include quantitative and qualitative performance targets in order to allow for timely monitoring so that appropriate corrective actions can be taken without undue delay if agreed service levels are not met.</p>	<p><b>Effective outsourcing agreements require service levels, and the targets must be tailored to the parties' requirements.</b></p> <ul style="list-style-type: none"> <li>Include service levels with quantitative and qualitative performance targets.</li> </ul>	
14.	Para 37 (j)	<p>The reporting obligations of the cloud service provider to the undertaking, including, as appropriate, the obligations to submit reports relevant for the undertaking's security function and key functions, such as reports of the internal audit function of the cloud service provider.</p>	<p><b>It is standard for outsourcing agreements to contain notification obligations but this requirement clarifies that service recipients may press for receipt of report for its internal audit function.</b></p> <ul style="list-style-type: none"> <li>Include an obligation on the cloud service provider to provide the reports relevant for the undertaking's internal audit function.</li> </ul>	
15.	Para 37 (k)	<p>Whether the cloud service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested.</p>	<p><b>Insurance in this setting is market practice and minimises risk for all parties.</b></p> <ul style="list-style-type: none"> <li>Specify whether cloud service provider's insurance is required / not required.</li> </ul>	
16.	Para 37 (l)	<p>The requirements to implement and test business contingency plans.</p>	<p><b>It is highly recommended for parties to an outsourcing to consider business contingency plans. It appears from this requirement that both parties must include in the agreement requirements to implement and test their respective business contingency plans.</b></p> <ul style="list-style-type: none"> <li>Include provisions regarding business contingency plans.</li> </ul>	
17.	Para 37 (m)	<p>The requirements for the cloud service provider to grant the undertaking, its supervisory authorities and any other person appointed by the undertaking or the supervisory authorities all required access rights set out in the column to the right:</p>	<p><b>The EIOPA Guidelines prescribe detailed and extensive access rights in favour of the undertaking, its appointees and supervisory authorities. Undertakings should pay close attention to ensure these are reflected in the agreement:</b></p> <ul style="list-style-type: none"> <li>Full access to all relevant business premises (head office and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel</li> </ul>	

	Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
			<p>and the cloud service provider's external auditors; and</p> <ul style="list-style-type: none"> <li>Unrestricted rights of inspection and auditing related to the cloud outsourcing arrangements, to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.</li> </ul>	
18.	Para 37 (n)	<p>Provisions that ensure that the data that are owned by the undertaking can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the cloud service provider.</p>	<p><b><i>While outsourcing agreements normally provide for these situations, this requirement should serve as a reminder for parties to include (i) sufficient IP and data ownership provisions and (ii) provisions detailing how to retain access to the data if the cloud service provider becomes insolvent or similar.</i></b></p> <ul style="list-style-type: none"> <li>Include accommodation for continued access to data, in case of cloud service provider's insolvency, resolution or discontinuation.</li> </ul>	
<b>Guideline 11 – Access and audit rights</b>				
19.	Para 38	<p>The cloud outsourcing agreement should not limit the undertaking's effective exercise of access and audit rights as well as control options on cloud services in order to fulfil its regulatory obligations.</p>	<p><b><i>This part of the EIOPA Guidelines reiterate the importance for undertakings to ensure that the outsourcing agreement, as a general comment, allows for broad audit rights by the undertaking.</i></b></p> <ul style="list-style-type: none"> <li>Include in the recitals and, if appropriate, a provision which makes clear that there shall be no limits on the undertaking's information, access and audit rights other than as expressly set out in the agreement.</li> </ul>	
20.	Para 39	<p>The undertaking should exercise its access and audit rights, determine the audit frequency and the areas and services to be audited on a risk-based approach, according to Section 8 of EIOPA Guidelines on System of Governance.</p>	<p><b><i>The right to audit the cloud service provider is common practice in outsourcing agreements. This requirement highlights that such rights need to be sufficiently flexible to accommodate any increased risk.</i></b></p> <ul style="list-style-type: none"> <li>Include a provision to ensure that the internal audit function can review the outsourced function, and make express reference to the requirement in Section 8 of EIOPA Guidelines on System of Governance.</li> </ul>	
21.	Para 40	<p>In determining the frequency and the scope of its exercise of access or audit rights, the undertaking should consider whether the cloud outsourcing is related to a critical</p>	<p><b><i>It is common in outsourcings for the parties to consider the frequency of audits. Undertakings must consider it with respect to its risk exposure to the cloud service provider, and it is advisable to do so at an early stage as part of the pre-outsourcing analysis.</i></b></p>	

Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
	or important operational function or activity, the nature and extent of risk and impact on the undertaking from the cloud outsourcing arrangements.	<ul style="list-style-type: none"> <li>Express clearly in the audit provisions the undertaking's required frequency of audits, for example, in terms of specific time periods (e.g., months or years) or on a general needs-basis.</li> </ul>	
22.	Para 41 If the exercise of its access or audit rights, or the use of certain audit techniques creates a risk for the environment of the cloud service provider and/or another cloud service provider's client (e.g., the impact on service levels, availability of data, confidentiality aspects), the undertaking and the cloud service provider should agree on alternative ways to provide a similar level of assurance and service to the undertaking (e.g., the inclusion of specific controls to be tested in a specific report/certification produced by the cloud service provider).	<p><b>Cloud service providers will likely raise issues with certain audit techniques. Parties to outsourcings may negotiate this point and should seek technical input as appropriate.</b></p> <ul style="list-style-type: none"> <li>Include audit provisions in the agreement that specify which audit techniques are acceptable and which are not acceptable.</li> <li>Ensure that the choice of audit techniques does not limit the scope of the audit in conflict with the other audit requirements of the EIOPA Guidelines.</li> </ul>	
23.	Para 42 <b>Without prejudice to their final responsibility regarding the activities performed by their cloud service providers, in order to use audit resources more efficiently and decrease the organisational burden on the cloud service provider and its customers, undertakings may use:</b>	<ul style="list-style-type: none"> <li>Depending on the nature of the agreement and the negotiations between the parties, and provided the undertaking's responsibility is not affected, include any of the relevant provisions of para 42, identified below:</li> </ul>	
24.	Para 42 (a) Third-party certifications and third-party or internal audit reports made available by the cloud service provider.	<ul style="list-style-type: none"> <li>Include third-party certifications.</li> <li>Include third-party or internal audit reports.</li> </ul>	
25.	Para 42 (b) Pooled audits (i.e., performed jointly with other clients of the same cloud service provider), or pooled audits performed by a third party appointed by them.	<ul style="list-style-type: none"> <li>Include pooled audits with other clients of the same cloud service provider.</li> <li>Include third-party audit.</li> </ul>	
26.	Para 43 <b>In case of cloud outsourcing of critical or important operational functions or activities, undertakings should make use of the method referred to in paragraph 42(a) only if they:</b>	<ul style="list-style-type: none"> <li>Where using the certifications and reports described in para 42(a), all the requirements of para 43 identified below (presuming the outsourcing relates to a critical or important function or activity):</li> </ul>	



	Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
27.	Para 43 (a)	Ensure that the scope of the certification or the audit report covers the systems (e.g., processes, applications, infrastructure, data centres, etc.) and the controls identified by the undertaking and assesses the compliance with relevant regulatory requirements.	<p><b><i>The undertaking should include these requirements as required conditions for any certification or audit report.</i></b></p> <ul style="list-style-type: none"> <li>• Ensure the certifications or reports in the agreement cover all relevant systems, key controls and regulatory requirements.</li> </ul>	
28.	Para 43 (b)	Thoroughly assess the content of the certifications or audit reports on a regular basis and verify that the certifications or reports are not obsolete.	<p><b><i>This requirement is in line with the obligation on undertakings to maintain responsibility as expected in an outsourcing agreement. Importantly, this requirement may limit the undertakings' ability to agree to full reliance on the certifications or reports in the outsourcing agreement.</i></b></p> <ul style="list-style-type: none"> <li>• Include an assessment mechanism for the content and status of certifications or audits.</li> </ul>	
29.	Para 43 (c)	Ensure that key systems and controls are covered in future versions of the certification or audit report.	<p><b><i>In line with the above requirements, the parties may ensure compliance by specifying this as conditions in the outsourcing agreement.</i></b></p> <ul style="list-style-type: none"> <li>• Ensure in the agreement that future reports include key systems and controls.</li> </ul>	
30.	Para 43 (d)	Are satisfied with the aptitude of the certifying or auditing party (e.g., with regard to rotation of the certifying or auditing company, qualifications, expertise, performance/verification of the evidence in the underlying audit file).	<p><b><i>In line with the above requirements, the parties may ensure compliance by specifying this as conditions in the outsourcing agreement.</i></b></p> <ul style="list-style-type: none"> <li>• Include clear requirements for satisfactory aptitude of certifying or auditing third party.</li> </ul>	
31.	Para 43 (e)	Are satisfied that the certifications are issued and the audits are performed according to appropriate standards and include a test of the operational effectiveness of the key controls in place.	<p><b><i>In line with the above requirements, the parties may ensure compliance by specifying this as conditions in the outsourcing agreement.</i></b></p> <ul style="list-style-type: none"> <li>• Include clear requirements to ensure certificates or audits meet recognised professional standards and include a test of the key controls.</li> </ul>	
32.	Para 43 (f)	Have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification should be	<p><b><i>In line with the above requirements, the parties may ensure compliance by specifying this as conditions in the outsourcing agreement.</i></b></p> <ul style="list-style-type: none"> <li>• Include reasonable right for undertaking to request an expanded scope of the certifications or reports.</li> </ul>	

	Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
		reasonable and legitimate from a risk management perspective.		
33.	Para 43 (g)	Retain the contractual right to perform individual on-site audits at their discretion with regard to the cloud outsourcing of critical or important operational functions or activities; such right should be exercised in case of specific needs not possible through other types of interactions with the cloud service provider.	<p><b><i>It is expected in an outsourcing agreement to retain some right to perform an audit in place of a certification or other third-party mechanism but the circumstances of when such a right would be triggered may be negotiated. This requirement under the EIOPA Guidelines clarifies that the audit should largely be at the undertaking's discretion. It is therefore important that this is reflected in the drafting of the outsourcing agreement.</i></b></p> <ul style="list-style-type: none"> <li>• Include right for undertaking to perform an on-site audit at discretion, or to the extent of such discretion, under the EIOPA Guidelines.</li> </ul>	
34.	Para 44	For outsourcing to cloud service providers of critical or important operational functions, the undertaking should assess whether third-party certifications and reports as referred to in paragraph 42(a) are adequate and sufficient to comply with its regulatory obligations and, on a risk-based approach, should not rely solely on these reports and certificates over time.	<p><b><i>This provision serves as a reminder to undertakings to ensure that they meet their regulatory obligations without overly relying on third-party certifications and reports in relation to outsourcings of critical or important operational functions.</i></b></p> <ul style="list-style-type: none"> <li>• Verify that there are sufficient internal mechanisms in place to meet the regulatory obligations independently of the third-party certifications or reports obtained under the outsourcing agreement.</li> <li>• If appropriate, include alternative measures for the undertaking to ascertain that it meets its regulatory obligations.</li> </ul>	
35.	Para 45	Before a planned on-site visit, the party to exercise its right of access (undertaking, auditor or third party acting on behalf of the undertaking(s)) should provide prior notice in a reasonable time period, unless an early prior notification has not been possible due to an emergency or crisis situation. Such notice should include the location and purpose of the visit and the personnel that will participate in the visit.	<p><b><i>This requirement conforms with the provisions normally seen in outsourcing agreements.</i></b></p> <ul style="list-style-type: none"> <li>• Include clear requirement for notice in a reasonable time period prior to on-site visit, unless emergency or crisis.</li> <li>• Specify that the notice must include details of the location, purpose of the visit and all personnel that will participate.</li> </ul>	
36.	Para 46	Considering that cloud solutions have a high level of technical complexity, the undertaking should	<b><i>Outsourcing agreements normally contain a provision to this effect. This requirement</i></b>	

Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes	
	verify that the staff performing the audit – being its internal auditors or the pool of auditors acting on its behalf, or the cloud service provider’s appointed auditors – or, as appropriate, the staff reviewing the third-party certification or service provider’s audit reports have acquired the appropriate skills and knowledge to perform the relevant audits and/or assessments.	<p><i>should therefore be a guiding point for drafting such provisions.</i></p> <ul style="list-style-type: none"> <li>• Include clear requirements to ensure the person performing the audit has appropriate skills and knowledge.</li> </ul>		
<b>Guideline 12 – Security of data and systems</b>				
37.	Para 47	<p>The undertaking should ensure that cloud service providers comply with European and national regulations as well as appropriate ICT security standards.</p>	<p><b><i>Addressing IT security standards has become increasingly important and common since the introduction of privacy laws such as the GDPR. The undertaking should include an appropriate contractual obligation on the cloud service provider and be prepared to monitor compliance on an ongoing basis.</i></b></p> <ul style="list-style-type: none"> <li>• Include an obligation on the cloud service provider to comply with European and national regulations, and ICT security standards.</li> <li>• Include defined data and system security requirements and monitor compliance.</li> </ul>	
38.	Para 48	<p>In case of outsourcing of critical or important operational functions or activities to cloud service providers, the undertaking should additionally define specific information security requirements in the outsourcing agreement and monitor compliance with these requirements on a regular basis.</p>	<ul style="list-style-type: none"> <li>• Ensure that the outsourcing agreement defines specific information security requirements, and monitor compliance with these requirements on a regular basis.</li> </ul>	
39.	Para 49	<p><b>For the purposes of paragraph 48, in case of outsourcing of critical or important operational functions or activities to cloud service providers, the undertaking, applying a risk-based approach, and taking into account its responsibilities and those of the cloud service provider, should:</b></p>	<p><b><i>Depending on the outcome of the pre-outsourcing risk assessment and the negotiations between the parties, in respect of outsourcing of critical or important functions or activities, undertakings should consider whether to include in the outsourcing agreement provisions in respect of any of the relevant requirements of para 49 identified below:</i></b></p>	
40.	Para 49 (a)	<p>Agree on clear roles and responsibilities between the cloud</p>	<ul style="list-style-type: none"> <li>• Assign in the agreement clear roles and responsibilities between the cloud</li> </ul>	

Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
	service provider and the undertaking in relation to the operational functions or activities affected by the cloud outsourcing, which should be clearly split.	<p>service provider and the undertaking in relation to each outsourced function or activity.</p> <ul style="list-style-type: none"> <li>Clearly split these roles and responsibilities (i.e., avoid joint roles and responsibilities).</li> </ul>	
41. Para 49 (b)	Define and decide on an appropriate level of protection of confidential data, continuity of activities outsourced, integrity and traceability of data and systems in the context of the intended cloud outsourcing.	<ul style="list-style-type: none"> <li>Define and specify an appropriate level of protection of confidential data, continuity of services, and data and systems' integrity and traceability.</li> </ul>	
42. Para 49 (c)	Consider specific measures where necessary for data in transit, data in memory and data at rest; for example, the use of encryption technologies in combination with an appropriate keys management.	<ul style="list-style-type: none"> <li>Define specific measures for data in transit, data in memory and data at rest (e.g., encryption technologies, key management and/or appropriate user and access management).</li> </ul>	
43. Para 49 (d)	Consider the mechanisms of integration of the cloud services with the systems of the undertakings, for example, the Application Programming Interfaces and a sound user and access management process.	<ul style="list-style-type: none"> <li>Consider internally and, if necessary, reflect in the agreement, the mechanisms of integration of the cloud services with the systems of the undertakings.</li> </ul>	
44. Para 49 (e)	Contractually ensure that network traffic availability and expected capacity meet strong continuity requirements, where applicable and feasible.	<ul style="list-style-type: none"> <li>Where applicable and feasible, define and require the appropriate network traffic availability and expected capacity.</li> </ul>	
45. Para 49 (f)	Define and decide on proper continuity requirements ensuring adequate levels at each level of the technological chain, where applicable.	<ul style="list-style-type: none"> <li>Where applicable, define appropriate and proper continuity requirements at each level of the technological chain.</li> </ul>	
46. Para 49 (g)	Have a sound and well documented incident management process including the respective responsibilities, for example, by the definition of a cooperation model in case of actual or suspected incidents occur.	<ul style="list-style-type: none"> <li>In relation to both parties, define specific incident management processes relevant to the management of actual or suspected incidents (e.g., personal data breach or denial-of-service attack). This should entail appropriate assignment of responsibility for each process and may include a cooperation model.</li> </ul>	

	Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
47.	Para 49 (h)	Adopt a risk-based approach to data storage and data processing locations(s) (i.e., country or region) and information security considerations.	<ul style="list-style-type: none"> <li>Consider including any agreed data residency policy in the outsourcing agreement (e.g., as a schedule) and the appropriate frequency of review of the policy.</li> <li>Ensure the outsourcing agreement's audit provisions are aligned with the requirement for the undertaking to verify the cloud service provider's compliance with this provision.</li> </ul>	
48.	Para 49 (i)	Monitor the fulfilment of the requirements relating to the effectiveness and efficiency of control mechanisms implemented by the cloud service provider that would mitigate the risks related to the provided services.	<ul style="list-style-type: none"> <li>Ensure the appropriate level of fulfilment is reflected in the outsourcing agreement.</li> <li>Ensure the outsourcing agreement's audit provisions enable the undertaking to monitor the cloud service provider's fulfilment of the requirements relating to the effectiveness and efficiency of control mechanisms.</li> </ul>	
<b>Guideline 13 – Sub-outsourcing of critical or important operational functions or activities</b>				
49.	Para 50	<b>If sub-outsourcing of critical or important operational functions (or a part thereof) is permitted, the cloud outsourcing agreement between the undertaking and the cloud service provider should:</b>	<b><i>If the cloud outsourcing agreement relates to critical or important operational functions and permits sub-outsourcing, the parties are expected to include all the requirements of para 50 below:</i></b>	
50.	Para 50 (a)	Specify any types of activities that are excluded from potential sub-outsourcing.	<p><b><i>An outsourcing agreement for critical or important functions needs to be clear on whether and to what extent the subcontracting of any/all of the obligations/services of the cloud service provider are permitted:</i></b></p> <ul style="list-style-type: none"> <li>Ensure the agreement makes clear which elements of the services can/cannot be subcontracted (e.g., the clause may include various materiality thresholds by reference to the criticality/risk of the service being outsourced, below which subcontracting is permitted without additional consent).</li> </ul>	
51.	Para 50 (b)	Indicate the conditions to be complied with in case of sub-outsourcing (e.g., that the sub-outsourcer will also fully comply with the relevant obligations of the cloud service provider). These	<b><i>The effect of this provision is that the EIOPA Guidelines only permit undertakings to allow sub-outsourcing if any sub-outsourcer also complies with the terms of the outsourcing.</i></b>	



	Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
		obligations include the audit and access rights and the security of data and systems.	<ul style="list-style-type: none"> <li>• Include any appropriate conditions of the sub-outsourcing.</li> <li>• Ensure that the outsourcing agreement contains an obligation on the cloud service provider to impose the same terms on any sub-outsourcer (including, specifically, the audit and access rights and the security of data and systems).</li> </ul>	
52.	Para 50 (c)	Indicate that the cloud service provider retains full accountability and oversight for the services sub-outsourced.	<p><b><i>As per good practice, parties should consider what types of activities they would be comfortable with being sub-outsourced, keeping in mind the overarching requirements of the EIOPA Guidelines. This requirement also imposes a de facto monitoring obligation on the cloud service provider vis-à-vis the sub-outsourcer.</i></b></p> <ul style="list-style-type: none"> <li>• Include an obligation on the cloud service provider to retain accountability and to oversee sub-outsourced services in light of the outsourcing agreement's terms.</li> </ul>	
53.	Para 50 (d)	include an obligation for the cloud service provider to inform the undertaking of any planned significant changes to the sub-contractors or the sub-outsourced services that might affect the ability of the service provider to meet its obligations under the cloud outsourcing agreement. The notification period for those changes should allow the undertaking, at least, to carry out a risk assessment of the effects of the proposed changes before the actual change in the sub-outsourcers or the sub-outsourced services comes into effect.	<p><b><i>It is customary to include in the outsourcing agreement a notification obligation for these types of changes. It is notable that this requirement expressly requires the notification period, normally a point of negotiation, to be long enough for risk assessment and objection. This may favour the undertaking.</i></b></p> <ul style="list-style-type: none"> <li>• Include an obligation on the cloud service provider to inform of any planned significant changes to the sub-outsourcing or services.</li> <li>• Ensure any related notification period in the agreement is long enough to allow for risk assessment and objection by the undertaking.</li> </ul>	
54.	Para 50 (e)	Ensure, in cases where a cloud service provider plans changes to a sub-outsourcer or sub-outsourced services that would have an adverse effect on the risk assessment of the agreed services, that the undertaking has the right to object to such changes and/or the right to terminate and exit the contract.	<p><b><i>The right for the undertaking to object or terminate would normally be considered in discussions around sub-outsourcing. While this seemingly provides a right for undertakings to object or terminate, the undertakings' right may be limited by having to demonstrate that the change would have an adverse effect.</i></b></p> <ul style="list-style-type: none"> <li>• Include the right for undertaking to object or terminate, in case of changes to sub-outsourcing that would have an adverse effect.</li> </ul>	

Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
		<ul style="list-style-type: none"> <li>Ensure the termination provisions are aligned and accordingly allow for termination in these circumstances.</li> </ul>	
<b>Guideline 15 – Termination rights and exit strategies</b>			
55.	Para 55	<p>In case of cloud outsourcing of critical or important operational functions or activities, within the cloud outsourcing agreement, the undertaking should have a clearly defined exit strategy clause ensuring that it is able to terminate the arrangement, where necessary. The termination should be made possible without detriment to the continuity and quality of its provision of services to policyholders. To achieve this, the undertaking should:</p>	<p><i>The requirement for undertakings to be able to terminate outsourcings of critical or important operational functions or activities where necessary will likely entail extensive negotiations between the parties.</i></p> <p><i>Depending on the negotiations between the parties, undertakings should consider whether to include in the outsourcing agreement provisions in respect of any of the relevant requirements of para 55 identified below:</i></p>
56.	Para 55 (a)	Develop exit plans that are comprehensive, service-based, documented and sufficiently tested (e.g., by carrying out an analysis of the potential costs, impacts, resources and timing implications of the various potential exit options).	<ul style="list-style-type: none"> <li>Ensure the termination provisions in the agreement reflect the undertaking's exit plans.</li> </ul>
57.	Para 55 (b)	Identify alternative solutions and develop appropriate and feasible transition plans to enable the undertaking to remove and transfer existing activities and data from the cloud service provider to alternative service providers or back to the undertaking. These solutions should be defined with regard to the challenges that may arise because of the location of data, taking the necessary measures to ensure business continuity during the transition phase.	<ul style="list-style-type: none"> <li>Ensure the undertaking has control of its preferred solution and set an appropriate level of discretion for any such decisions.</li> </ul>
58.	Para 55 (c)	Ensure that the cloud service provider adequately supports the undertaking when transferring the outsourced data, systems or applications to another service	<ul style="list-style-type: none"> <li>Include an obligation on the cloud service provider to provide support on request.</li> <li>Consider the cost implications of the support and how the parties wish to apportion such costs.</li> </ul>

	Guidelines Ref.	Description of Requirement	General Comments / How to Meet the Requirement	Notes
		provider or directly to the undertaking.		
59.	Para 55 (d)	Agree with the cloud service provider that once retransferred to the undertaking, its data will be completely and securely deleted by the cloud service provider in all regions.	<ul style="list-style-type: none"> <li>• Include an obligation on the cloud service provider to delete the undertaking's data upon the undertaking's request.</li> </ul>	

# SCHEDULE 4

## UK SPECIFIC REGULATION

	Ref.	Description of Requirement	General Comments / How to Meet the Requirement
The FCA Principles			
1.	PRIN 2.1.1	<ul style="list-style-type: none"> <li>• The FCA Principles are applicable to all FCA regulated firms. When outsourcing to another firm, an authorised firm must be aware of the effects of outsourcing on its obligations under the FCA Principles and ensure that it continues to comply with the requirements. The FCA Principles are as follows:               <ol style="list-style-type: none"> <li>1. <b>Integrity</b> A firm must conduct its business with integrity.</li> <li>2. <b>Skill, care and diligence</b> A firm must conduct its business with due skill, care and diligence.</li> <li>3. <b>Management and control</b> A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.</li> <li>4. <b>Financial prudence</b> A firm must maintain adequate financial resources.</li> <li>5. <b>Market conduct</b> A firm must observe proper standards of market conduct.</li> <li>6. <b>Customers' interests</b> A firm must pay due regard to the interests of its customers and treat them fairly.</li> <li>7. <b>Communications with clients</b> A firm must pay due regard to the information needs of its clients, and communicate information to them in a way which is clear, fair and not misleading.</li> </ol> </li> </ul>	<p>Outsourcing failures have most commonly been found to constitute a breach of Principle 3 (Management and Control) (see page 11). Other FCA Principles that have been cited in enforcement action for outsourcing failings include, Principle 2 (Skill, Care and Diligence), Principle 6 (Customers' Interests) and Principle 10 (Clients' Assets). To mitigate the risks of enforcement as a result of outsourcing failings, firms should ensure that:</p> <ul style="list-style-type: none"> <li>• They adhere to all applicable specific outsourcing rules and guidelines including, but not limited to, the EBA Guidelines, the EIOPA Guidelines, SMCR, and SYSC.</li> <li>• They adhere to the general spirit of the FCA Principles in relation to their outsourcing arrangements, in addition to complying with specific rules and guidance.</li> <li>• Adequate policies and procedures are in place to monitor outsourcing, and risks resulting from outsourcing.</li> <li>• Appropriate channels of reporting and escalation are established and publicised to employees.</li> <li>• All relevant employees and managers, so that each fully understands the firm's obligations under the FCA Principles.</li> <li>• All managers and relevant employees acknowledge and understand the broad reach of the FCA Principles (e.g., their use in enforcement (see Section 11.6)).</li> <li>• Accurate record-keeping is maintained to evidence the firm's compliance with the FCA Principles.</li> </ul>

Ref.	Description of Requirement	General Comments / How to Meet the Requirement
	<p>8. <b>Conflicts of interest</b> A firm must manage conflicts of interest fairly, both between itself and its customers and between a customer and another client.</p> <p>9. <b>Customers: relationships of trust</b> A firm must take reasonable care to ensure the suitability of its advice and discretionary decisions for any customer who is entitled to rely on its judgment.</p> <p>10. <b>Clients' assets</b> A firm must arrange adequate protection for clients' assets when it is responsible for them.</p> <p>11. <b>Relations with regulators</b> A firm must deal with its regulators in an open and cooperative way, and must disclose to the FCA appropriately anything relating to the firm of which that regulator would reasonably expect notice</p>	

### The PRA Principles

2.	Fundamental Rules Part of the PRA Rulebook, Rule 2	<ul style="list-style-type: none"> <li>The PRA Principles are applicable to all PRA regulated firms. When outsourcing to another firm, a PRA authorised firm must be aware of the effects of outsourcing on its obligations under the PRA Principles and ensure that it continues to comply with the requirements. The PRA Principles are as follows:             <ol style="list-style-type: none"> <li>A firm must conduct its business with integrity.</li> <li>A firm must conduct its business with due skill, care and diligence.</li> <li>A firm must act in a prudent manner.</li> <li>A firm must at all times maintain adequate financial resources.</li> </ol> </li> </ul>	<p>In particular, outsourcing failures have been found to constitute a breach of PRA Principles 2 (Due Skill, Care, and Diligence), 5 (Risk Management) and 6 (Control) (see Section 11.6). To mitigate the risks of enforcement as a result of outsourcing failings, firms should ensure that:</p> <ul style="list-style-type: none"> <li>They adhere to all applicable specific outsourcing rules and guidelines including, but not limited to, the EBA Guidelines, the EIOPA Guidelines, SMCR and the Outsourcing Part of the PRA Rulebook.</li> <li>In addition to complying with specific rules and guidance, they adhere to the general spirit of the PRA Principles in relation to their outsourcing arrangements.</li> <li>Adequate policies and procedures are in place to monitor outsourcing, and risks resulting from outsourcing.</li> <li>Appropriate channels of reporting and escalation are established and publicised to employees.</li> </ul>
----	--	---	--



Ref.	Description of Requirement	General Comments / How to Meet the Requirement
	<p>5. A firm must have effective risk strategies and risk management systems.</p> <p>6. A firm must organise and control its affairs responsibly and effectively.</p> <p>7. A firm must deal with its regulators in an open and co-operative way, and must disclose to the PRA appropriately anything relating to the firm of which the PRA would reasonably expect notice.</p> <p>8. (8) A firm must prepare for resolution so that, if the need arises, it can be resolved in an orderly manner with a minimum disruption of critical services.</p>	<ul style="list-style-type: none"> <li>• Appropriate training is provided to all relevant employees and managers, so that each fully understands the firm's obligations under the PRA Principles.</li> <li>• All managers and relevant employees acknowledge and understand the broad reach of the PRA Principles (e.g., their use in enforcement (see page 8))</li> <li>• Accurate record-keeping is maintained to evidence the firm's compliance with the PRA Principles.</li> </ul>

### Senior Managers and Certification Regime

3.	SYSC 24.2.6	<ul style="list-style-type: none"> <li>• Each firm needs to assess whether a particular outsourcing contract touches any of the Senior Manager Prescribed Responsibilities that apply to that firm.</li> <li>• If so, the Senior Managers with Prescribed Responsibilities will need to have oversight of the outsourced activities to ensure that they are fully satisfying their own Prescribed Responsibilities.</li> <li>• Senior Managers must also be mindful of where their individual areas of responsibility are affected by outsourcing. Senior Managers will be held accountable for failings in their area of responsibility.</li> </ul>	<p>A firm should:</p> <ul style="list-style-type: none"> <li>□ Consider how it will manage oversight of outsourced activities to ensure that its responsibilities are satisfied.</li> <li>• Ensure that the outsourcing agreement contains written designation of responsibility to ensure accountability for compliance with the relevant firm policies and FCA/PRA requirements, for example, in relation to remuneration, CASS or whistleblowing.</li> <li>• Ensure that there are suitable policies for the training of staff and managers within the service provider, in particular in relation to the requirements of the SMCR.</li> <li>• Ensure that the outsourcing agreement contains an obligation on the service provider to make available to both the outsourcing firm and the relevant regulators all necessary documentation, either to evidence compliance with policies and regulatory requirements, or to report to the regulators as required.</li> <li>• Ensure that there are sufficient resources available to Senior Managers to enable them to oversee the activities of the service provider effectively.</li> <li>• Put in place a process by which the service provider can report to the Senior Manager on the implementation of policies.</li> </ul>
----	-------------	--	---

Ref.	Description of Requirement	General Comments / How to Meet the Requirement
		<ul style="list-style-type: none"> <li>Ensure that the service provider is made aware of any views expressed by the regulatory bodies and any steps taken by them in relation to the outsourced activities.</li> </ul> <p>Senior Managers should:</p> <ul style="list-style-type: none"> <li>Consider what areas of outsourcing they could be responsible for.</li> <li>Ensure that they are adequately overseeing the implementation and ongoing functioning of outsourced services for which they are responsible.</li> <li>Ensure that they, and their subordinates, are well trained in their responsibilities and obligations in relation to outsourced services.</li> </ul>
4.	SUP 10C.10.6-7	<ul style="list-style-type: none"> <li>When outsourcing to another authorised firm, a firm must take reasonable care in ensuring that the service provider is contractually bound to ensure that any relevant senior management functions are performed by an FCA-approved Senior Manager.</li> <li>When a firm outsources a service to another member of the same group (each having its registered office in the UK), the firm will perform an FCA controlled function only if the function is performed under an arrangement entered into by the firm or if: (i) there is a contract between the firm and the relevant group member permitting this; and (ii) the function is performed under an arrangement entered into by the contractor.</li> <li>When outsourcing to a company which is not authorised, the outsourcing firm retains responsibility for any activity outsourced; further, the firm will need to ensure that any outsourced functions are overseen by an FCA approved Senior Manager.</li> </ul> <p>This provision addresses the question of which individuals may require approval under the SMCR when services are outsourced to another firm.</p> <p>The firm should consider:</p> <ul style="list-style-type: none"> <li>Who may need approval as a result of the outsourcing arrangements;</li> <li>Which of its Senior Managers is accountable for outsourced functions;</li> <li>Whether the outsourcing contract clearly states the respective responsibilities of the parties; and</li> <li>Whether the firm has sufficient oversight over the performance of outsourced functions.</li> </ul>
5.	4.1(21), Allocation of	<ul style="list-style-type: none"> <li>For PRA regulated firms the "responsibility for the firm's</li> </ul> <p>The firm should consider:</p>

	Ref.	Description of Requirement	General Comments / How to Meet the Requirement
	Responsibilities Part of the PRA Rulebook	performance of its obligations under Outsourcing” is a Prescribed Responsibility and will need to be assigned to a Senior Manager.	<ul style="list-style-type: none"> <li>Which Senior Manager is best placed to be assigned this function (given that the outsourced activities may range from IT outsourcing to outsourcing of a regulated activity); and</li> <li>Whether any internal oversight programme is required to assist the designated Senior Manager in fulfilling their Prescribed Responsibility.</li> </ul>
<b>Systems and Controls Rules (“SYSC” chapter of the FCA Handbook)</b>			
6.	SYSC 3.2.4	<ul style="list-style-type: none"> <li>A firm (i.e., an authorised person) cannot contract out its regulatory obligations and should therefore take reasonable care to supervise the discharge of outsourced functions.</li> <li>A firm should take steps to obtain sufficient information from its contractor to be able to assess the impact of outsourcing on its systems and controls.</li> </ul>	<p>The nature and extent of the systems and controls which a firm will need to maintain depends on a variety of factors, including the:</p> <ol style="list-style-type: none"> <li>Nature, scale and complexity of its business;</li> <li>Diversity of its operations, including geographical diversity;</li> <li>Volume and size of its transactions; and</li> <li>Degree of risk associated with each area of its operation.</li> </ol> <p>Firms should:</p> <ul style="list-style-type: none"> <li>Ensure that they have allocated sufficient resources to enable the effective supervision of the contractor.</li> <li>Ensure that the outsourcing agreement obliges the contractor to provide sufficient information to the outsourcing firm in relation to its systems and controls.</li> <li>Carry out regular reviews of the information from contractors, and of the policies and processes that are in place to ensure compliance.</li> </ul>
7.	SYSC 8.1.1	<p>A common platform firm (i.e., BIPRU, IFPRU, designated investment, exempt CAD, or investment firms, banks, building societies and dormant account fund operators) must:</p> <ul style="list-style-type: none"> <li>Ensure that it takes reasonable steps to avoid undue additional operational risk when relying on a third party for the performance of operational functions which are critical for the performance of regulated activities, listed activities or ancillary services on a continuous and satisfactory basis.</li> </ul>	<p>The service provider should have the ability, capacity, and any authorisation required by law to perform the outsourced functions, services or activities reliably and professionally. To ensure this, the outsourcing firm should:</p> <ul style="list-style-type: none"> <li>Carry out full due diligence on the service provider prior to entering into any agreement. In addition, the agreement should contain guarantees from the service provider in relation to their ability, capacity, and authorisation to perform the function, and there should be measures in place to ensure that the outsourcing firm can monitor this going forward.</li> </ul>

Ref.	Description of Requirement	General Comments / How to Meet the Requirement
	<ul style="list-style-type: none"> <li>• Not undertake the outsourcing of important operational functions in such a way as to impair materially:               <ul style="list-style-type: none"> <li>i. The quality of its internal control; and</li> <li>ii. (The ability of the FCA to monitor the firm's compliance with all obligations under the regulatory system and, if different, of a competent authority to monitor the firm's compliance with all obligations under MiFID II.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Establish methods for assessing the standard of performance of the service provider.</li> <li>• Ensure that a plan is in place for taking appropriate action if the service provider does not carry out the functions effectively and in compliance with applicable laws and regulatory requirements.</li> <li>• Ensure that it has retained the necessary expertise to supervise the outsourced functions effectively.</li> <li>• Ensure that it has the capacity to terminate the outsourcing arrangement without detriment to the continuity and quality of its provision of services to clients.</li> <li>• Ensure that the outsourcing agreement contains an obligation on the service provider to cooperate with the FCA and any other competent authority in connection with the outsourced activities. This includes ensuring that the service provider is obliged to provide to the FCA and any other relevant competent authority effective access to data related to the outsourced activities, and to the business premises of the service provider.</li> <li>• Put in place appropriate protections to ensure that the service provider protects any confidential information relating to the firm and its clients.</li> <li>• Establish, implement and maintain a contingency plan for disaster recovery and periodic testing of backup facilities for the outsourced activities.</li> </ul> <p>The outsourcing agreement should:</p> <ul style="list-style-type: none"> <li>• Contain an obligation on the service provider to disclose to the outsourcing firm any development that may have a material impact on its ability to carry out the outsourced functions effectively and in compliance with the applicable laws and regulatory requirements.</li> </ul>
8.	SYSC 8.1.3	<ul style="list-style-type: none"> <li>• Where a firm relies on a third party for the performance of operational functions which are not critical or important for the performance of relevant services and activities on a continuous and satisfactory basis, it should take into account, in a manner that is proportionate given the nature, scale and complexity of the outsourcing, the rules in</li> </ul> <ul style="list-style-type: none"> <li>• SYSC 4.1.1 R requires a firm to have effective processes to identify, manage, monitor and report risks and internal control mechanisms.</li> <li>• In order to comply with the SYSC 4.1.1 R requirement, a firm should consider the rules and guidance in this section, even when the function outsourced is not critical or important.</li> </ul>

	Ref.	Description of Requirement	General Comments / How to Meet the Requirement
		SYSC 8 when complying with SYSC 4.1.1R.	
9.	SYSC 8.1.8	A UCITS investment firm must take the necessary steps to ensure that the conditions of Article 31(2) MiFID II Delegated Regulation are satisfied.	<ul style="list-style-type: none"> <li>UCITS firms should be prudent to ensure that each of the necessary steps as set out under the 'Internal governance/overarching requirements' heading in the MiFID II Commission Delegated Regulation section of Part Two are satisfied.</li> </ul>
10.	SYSC 8.1.12	<ul style="list-style-type: none"> <li>A firm should notify the FCA when it intends to rely on a third party for the performance of operational functions which are critical or important for the performance.</li> </ul>	<ul style="list-style-type: none"> <li>The firm should consider whether this obligation should be formalised within a policy, and/or whether standard notification wording should be produced.</li> </ul>
11.	SYSC 8.1.13	<ul style="list-style-type: none"> <li>A UCITS management company must retain the necessary resources and expertise so as to monitor effectively the activities carried out by third parties on the basis of an arrangement with the firm, especially with regard to the management of the risk associated with those arrangements.</li> </ul>	<ul style="list-style-type: none"> <li>Firms should consider providing training to enable management and staff to determine where risks arise in relation to the outsourced activities.</li> </ul>
12.	SYSC 13.9.2	<ul style="list-style-type: none"> <li>Insurers should take particular care to manage material outsourcing arrangements and a firm should notify the FCA when it intends to enter into a material outsourcing arrangement.</li> </ul>	<ul style="list-style-type: none"> <li>The insurer should consider whether this obligation should be formalised within a policy, and/or whether standard notification wording should be produced.</li> </ul>
13.	SYSC 13.9.3	<ul style="list-style-type: none"> <li>Insurers should not assume that because a service provider is either a regulated firm or an intra-group entity an outsourcing arrangement with that provider will, in itself, necessarily imply a reduction in operational risk.</li> </ul>	<ul style="list-style-type: none"> <li>Due diligence measures should be applied regardless of the nature of the service provider.</li> </ul>
14.	SYSC 13.9.4	<p>Before entering into, or significantly changing, an outsourcing arrangement, an insurer should:</p> <ul style="list-style-type: none"> <li>Analyse how the arrangement will fit with its organisation and reporting structure, business strategy, overall risk profile and ability to meet its regulatory obligations;</li> </ul>	<ul style="list-style-type: none"> <li>In its due diligence of service providers, the insurer should take into account: <ul style="list-style-type: none"> <li>i. Its business model, nature, scale, complexity, financial situation, ownership and group structure;</li> <li>ii. The long-term relationships with service providers that have already been assessed and that already perform services for the outsourcing firm;</li> <li>iii. Whether the service provider is a parent undertaking or subsidiary of the outsourcing firm, is part of the</li> </ul> </li> </ul>



Ref.	Description of Requirement	General Comments / How to Meet the Requirement
	<ul style="list-style-type: none"> <li>• Consider whether the agreements establishing the arrangement will allow it to monitor and control its operational risk exposure relating to the outsourcing;</li> <li>• Conduct appropriate due diligence of the service provider's financial stability and expertise;</li> <li>• Consider how it will ensure a smooth transition of its operations from its current arrangements to a new or changed outsourcing arrangement (including what will happen upon termination of the contract); and</li> <li>• Consider any concentration risk implications, such as the business continuity implications that may arise if a single service provider is used by several firms.</li> </ul>	<p>accounting scope of consolidation of the outsourcing firm, or is owned by firms that are members of the same institutional protection scheme;</p> <p>iv. Whether the service provider is supervised by a regulator.</p> <ul style="list-style-type: none"> <li>• Where the outsourcing involves the processing of personal or confidential data, the outsourcing firm should be satisfied that the service provider implements appropriate technical and organisational measures to protect the data.</li> <li>• Firms should make a risk assessment, taking into account the expected benefits and costs of the outsourcing arrangement, and operational risk including: <ul style="list-style-type: none"> <li>i. The risk from outsourcing to a dominant service provider that is not easily substitutable; and</li> <li>ii. Multiple outsourcing arrangements with the same service provider or closely connected service providers.</li> </ul> </li> </ul> <p>The risk assessment should take into account the risks associated with sub-outsourcing, including the additional risks that may arise if the sub-contractor is located in a third country or a different country from the service provider. Another potential issue is the risk that long and complex chains of sub-outsourcing will reduce the ability of the outsourcing firm or the regulator properly to supervise the activity.</p> <ul style="list-style-type: none"> <li>• During the risk assessment, the firm may also consider whether to: <ul style="list-style-type: none"> <li>i. Identify and classify the relevant functions and related data and systems as regards their sensitivity and required security measures;</li> <li>ii. Analyse the functions and related data and systems that are being considered for outsourcing or have been outsourced; the firm should also address the operational risks relating to legal, ICT, compliance and reputational risks;</li> <li>iii. Consider the consequences of where the service provider is located;</li> <li>iv. Consider the political stability and security situation of the jurisdictions in question;</li> <li>v. Define and decide on an appropriate level of protection of data confidentiality, of continuity of the activities outsourced and of the integrity and traceability of data and systems in the context of the intended outsourcing.</li> </ul> </li> </ul>
15.	SYSC 13.9.5	<p>In negotiating its contract with a service provider, an insurer should consider the following:</p> <ul style="list-style-type: none"> <li>• The firm should consider whether this approach to contract negotiation should be formalised within a policy.</li> </ul>

Ref.	Description of Requirement	General Comments / How to Meet the Requirement
	<ul style="list-style-type: none"> <li>• Reporting or notification requirements it may wish to impose on the service provider;</li> <li>• Whether sufficient access will be available to its internal auditors, external auditors or actuaries and to the FCA;</li> <li>• Information ownership rights, confidentiality agreements and information barriers to protect client and other information (including arrangements at the termination of the contract);</li> <li>• The adequacy of any guarantees and indemnities;</li> <li>• The extent to which the service provider must comply with the firm's policies and procedures (covering, for example, information security);</li> <li>• The extent to which a service provider will provide business continuity for outsourced operations, and whether exclusive access to its resources is agreed;</li> <li>• The need for continued availability of software following difficulty at a third-party supplier;</li> <li>• The processes for making changes to the outsourcing arrangement (e.g., changes in processing volumes, activities and other contractual terms) and the conditions under which the firm or service provider can choose to change or terminate the outsourcing arrangement, such as where there is one of the following: <ul style="list-style-type: none"> <li>i. A change of ownership or control (including insolvency or receivership) of the service provider or firm; or</li> <li>ii. Significant change in the business operations (including subcontracting) of the service provider or firm; or</li> <li>iii. Inadequate provision of services that may lead to the firm being unable to meet its regulatory obligations.</li> </ul> </li> </ul>	

	Ref.	Description of Requirement	General Comments / How to Meet the Requirement
16.	SYSC 13.9.6	<p>In implementing a relationship management framework, and drafting the service level agreement with the service provider, an insurer regards:</p> <ul style="list-style-type: none"> <li>• The identification of qualitative and quantitative performance targets to assess the adequacy of service provision, to both the firm and its clients, where appropriate;</li> <li>• The evaluation of performance through service delivery reports and periodic self-certification or independent review by internal or external auditors; and</li> <li>• Remedial action and escalation processes for dealing with inadequate performance.</li> </ul>	<ul style="list-style-type: none"> <li>• Insurers should ensure that the outsourcing agreement with the service provider contains an obligation on the service provider to provide service reports over a specified timeframe, and to submit to review by the outsourcing firm, internal or external auditors.</li> </ul>
17.	SYSC 13.9.7	<ul style="list-style-type: none"> <li>• In some circumstances, an insurer may wish to use externally validated reports commissioned by the service provider, to seek comfort as to the adequacy and effectiveness of its systems and controls. The use of such reports does not absolve the insurer of its responsibility to maintain other oversight.</li> <li>• In addition, the insurer should not have to forfeit its right to access, for itself or its agents, to the service provider's premises.</li> </ul>	<ul style="list-style-type: none"> <li>• Insurers should ensure that they have the ability to monitor the performance of a service provider to the extent that they can satisfy themselves that their oversight is sufficient.</li> </ul>
18.	SYSC 13.9.8	<ul style="list-style-type: none"> <li>• An insurer should ensure that it has appropriate contingency arrangements to allow business continuity in the event of a significant loss of services from the service provider.</li> </ul>	<ul style="list-style-type: none"> <li>• Continuity plans should take into account the possible event that the quality of the provision of the outsourced functions deteriorates to an unacceptable level or fails. Such plans should also take into account the potential impact of the insolvency or other failures of service providers and, where relevant, political risks in the service provider's jurisdiction.</li> <li>• Outsourcing firms should review all relevant information received from the service provider, including reports on business continuity measures and testing.</li> <li>• Outsourcing firms should have a documented exit strategy that takes into account the possibility of: <ul style="list-style-type: none"> <li>i. The termination of the outsourcing arrangements;</li> </ul> </li> </ul>

Ref.	Description of Requirement	General Comments / How to Meet the Requirement
		<ul style="list-style-type: none"> <li>ii. The failure of the service provider;</li> <li>iii. 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;</li> <li>iv. Material risks arising for the appropriate and continuous application of the function.</li> </ul> <ul style="list-style-type: none"> <li>• Outsourcing firms should identify alternative solutions and develop transition plans to enable them to remove outsourced functions and data from the service provider and transfer them to alternative providers or back to themselves.</li> <li>• When developing exit strategies, outsourcing firms should: <ul style="list-style-type: none"> <li>i. Define the objectives of the exit strategy;</li> <li>ii. Perform a business impact analysis that is commensurate with the risk of the outsourced processes, services or activities, with the aim of identifying what human and financial resources would be required to implement the exit plan and how much time it would take;</li> <li>iii. Assign roles, responsibilities and sufficient resources to manage exit plans and the transition of activities;</li> <li>iv. Define criteria for the successful transition of outsourced functions and data; and</li> <li>v. Define the indicators to be used for monitoring the outsourcing arrangement.</li> </ul> </li> </ul>

# SCHEDULE 5

## COMPARISON MIFID II DELEGATED REGULATION AND EBA GUIDELINES

Topic	MiFID II Delegated Regulation	EBA Guidelines	Comparison
<b>Definition of "critical or important" functions</b>	<p>A critical or important operational function is defined in MiFID II Delegated Regulation Article 30(1) as an operational function of which a defect of failure in performance would materially impair the continuing compliance of an investment firm with:</p> <ul style="list-style-type: none"> <li>a. the conditions and obligations of its authorisation or its other obligations under MiFID II;</li> <li>b. its financial performance; or</li> <li>c. the soundness or the continuity of its investment services and activities.</li> </ul>	<p>The definition in the EBA Guidelines is almost identical. Under the EBA Guidelines, a function should be seen as critical or important where a defect or failure in its performance would materially impair:</p> <ul style="list-style-type: none"> <li>a. the outsourcing firm's continuing compliance with the conditions of their authorisation or its other obligations under the CRD IV, Capital Requirements Regulation, the Payment Services Directive, or the E-Money Directive;</li> <li>b. the outsourcing firm's financial performance; or</li> <li>c. the soundness or continuity of their banking and payments services and activities.</li> </ul>	<p>The only distinction is therefore in condition (a) of each definition. However, since there is a general requirement in the MiFID II Delegated Regulation definition for continuing compliance with the obligations of the firm's authorisation, this should be read as including all of the legislation specified in the EBA Guidelines. This is confirmed by the EBA Guidelines, which state at Paragraph 31 that the definition of outsourcing has been fully aligned with the definition in the MiFID II Delegated Regulation.</p> <p>It would not be practical for institutions to apply different definitions for different activities (i.e., banking activities versus investment and payment services).</p>
<b>Further guidance on the definition of "critical or important" functions</b>	<p>Under the MiFID II Delegated Regulation Article 30(2), the following functions are not to be regarded as critical or important for the purposes of the definition in Article 30(1):</p> <ul style="list-style-type: none"> <li>a. the provision to the firm of advisory services, and other services which do not form part of the investment business of the firm, including the provision of legal advice, the training of personnel of the firm, billing services and the security of the firm's premises and personnel; and</li> <li>b. the purchase of standardised services, including market information services and the provision of price feeds.</li> </ul>	<p>The equivalent provision in the EBA Guidelines is at Paragraph 28, stating that, as a general principle, institutions and payment institutions should not consider as outsourcing:</p> <ul style="list-style-type: none"> <li>a. the acquisition of services that would otherwise not be undertaken by the institution or payment institution (e.g., advice from an architect);</li> <li>b. providing legal opinion and representation in front of the court and administrative bodies;</li> <li>c. cleaning, gardening and maintenance of the institution's or payment institution's premises;</li> <li>d. medical services;</li> <li>e. servicing of company cars;</li> </ul>	<p>The MiFID II Delegated Regulation and the EBA Guidelines both exclude the provision of legal advice and security services. However, the EBA Guidelines are more explicit in providing other exclusions. These are all likely to fall under the general exclusion in the MiFID II Delegated Regulation for "services which do not form part of the investment business of the firm". Explicit exclusions from the MiFID II Delegated Regulation are also absent from the EBA Guidelines (advisory service, personnel training, billing services). The absence of these services was noted in the responses to the EBA consultation (June-September 2018) ("the <b>Consultation Paper</b>"). The EBA responded (as noted above) that the definition of outsourcing has been fully aligned with the definition in the MiFID II Delegated Regulation.</p>



Topic	MiFID II Delegated Regulation	EBA Guidelines	Comparison
		<ul style="list-style-type: none"> <li>f. catering and vending machine services, clerical services;</li> <li>g. travel services;</li> <li>h. post-room services; or</li> <li>i. receptionists, secretaries and switchboard operators.</li> </ul> <p>Further guidance is given in the EBA Guidelines at Paragraph 31, which states that when assessing whether an outsourcing arrangement relates to a function that is critical or important, institutions should take into account:</p> <ul style="list-style-type: none"> <li>a. whether the outsourcing arrangement is directly connected to the provision of banking activities or payment services for which they are authorised;</li> <li>b. the potential impact of any disruption to the outsourced function; and</li> <li>c. the potential impact on their ability to identify, monitor and manage risk, comply with all legal and regulatory requirements, and conduct appropriate audits regarding the outsourced function.</li> </ul>	
<b>Retained responsibility of outsourcing firms</b>	<p>Under Article 31(1) of the MiFID II Delegated Regulation, investment firms outsourcing critical or important operational functions shall remain fully responsible for discharging all of their obligations under MiFID II and must comply with the following conditions:</p> <ul style="list-style-type: none"> <li>a. the outsourcing does not result in the delegation by senior management of its responsibility;</li> <li>b. the relationship and obligations of the investment firm towards its clients under the terms of MiFID II is not altered;</li> <li>c. the conditions with which the investment firm must comply in order to be authorised in accordance with Article 5 of MiFID II, and to</li> </ul>	<p>The equivalent provision from the EBA Guidelines is in Paragraph 5. This states that it is not permitted for an arrangement to provide for outsourcing that would:</p> <ul style="list-style-type: none"> <li>a. result in the delegation by the management body of its responsibility;</li> <li>b. alter the relationship and obligations of the institution or payment institution towards its clients;</li> <li>c. undermine the conditions of the institution or payment institution's authorisation; or</li> <li>d. remove or modify any of the conditions subject to which the institution or payment institution's</li> </ul>	<p>The provisions in the MiFID II Delegated Regulation and the EBA Guidelines are the same in substance and effect.</p>

Topic	MiFID II Delegated Regulation	EBA Guidelines	Comparison
	<p>remain so, are not undermined; and</p> <p>d. none of the other conditions, subject to which the firm's authorisation was granted is removed or modified.</p>	<p>authorisation was granted.</p>	

**Due diligence:** Both the MiFID II Delegated Regulation (Article 31(2)) and the EBA Guidelines (Paragraph 69) require firms to undergo a due diligence process before entering into an outsourcing arrangement. Under both the MiFID II Delegated Regulation and the EBA Guidelines, the outsourcing firm must ensure that the service provider has the ability, capacity, resources, organisational structure and the authorisations and regulatory permissions to perform the critical or important function. The following section sets out the obligations that the MiFID II Delegated Regulation and the EBA Guidelines require the outsourcing firm to place on the service provider.

<b>Due diligence: effective provision and legal compliance</b>	<p>Article 31(2)(b) of the MiFID II Delegated Regulation requires the outsourcing firm to take all necessary steps to ensure that the service provider carries out the outsourced services effectively and in compliance with applicable law and regulatory requirements, and to this end that the firm has established methods and procedures for assessing the standard of performance of the service provider and for reviewing on an ongoing basis the services provided by the service provider.</p>	<p>The equivalent applicable provision in the EBA Guidelines is at Paragraph 75(j), which requires that the outsourcing agreement should set out at least:</p> <ul style="list-style-type: none"> <li>a. the reporting obligations of the service provider to the institution or payment institution, including the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the critical or important function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements; and</li> <li>b. as appropriate, the obligations to submit reports of the internal audit function of the service provider.</li> </ul>	<p>Both the MiFID II Delegated Regulation and the EBA Guidelines require outsourcing firms to ensure that the service provider reports to the outsourcing firm with regards to the standard of service provided and the compliance by the service provider with applicable law and regulatory requirements.</p> <p>The final requirement in the EBA Guidelines is for submission of reports of the internal audit function of the service provider<sup>24</sup>. The equivalent applicable requirement in the MiFID II Delegated Regulation is at Article 31(2)(i), requiring that the investment firm, its auditors and the relevant competent authorities have effective access to data related to the outsourced functions, as well as to the relevant business premises of the service provider where necessary for the purpose of effective oversight (see below on access to data).</p>
<b>Due diligence: supervision and risk management</b>	<p>Under Article 31(2)(c) of the MiFID II Delegated Regulation, the outsourcing firm is required to ensure that the service provider properly supervises the carrying out of the outsourced functions, and to adequately manage the risks associated with the outsourcing.</p>	<p>The equivalent provision in the EBA Guidelines is at Paragraph 36(e), which states that the management body is at all times fully responsible and accountable for overseeing the day-to-day management of the institution or payment institution, including the management of all risks associated with outsourcing. This is supplemented with regard to supervision by the service provider at Paragraph 37. This states that institutions and payment institutions should have adequate competence and sufficient and appropriately skilled resources to ensure appropriate management</p>	<p>The requirements of the MiFID II Delegated Regulation and the EBA Guidelines with regard to supervision and management of risk are therefore aligned.</p>

<sup>24</sup> The internal audit function's responsibility is set out in Chapter 10 of the EBA Guidelines. 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, in particular, the outsourcing arrangements of critical or important functions.

Topic	MiFID II Delegated Regulation	EBA Guidelines	Comparison
		and oversight of outsourcing arrangements.	
<b>Disclosure obligations</b>	The MiFID II Delegated Regulation (Article 31(2)(f)) requires the outsourcing firm to ensure that the service provider has disclosed to the outsourcing firm any development that may have a material impact on its ability to carry out the outsourced functions effectively and in compliance with applicable laws and regulatory requirements.	Similarly, the EBA Guidelines (Paragraph 75(j)) require an outsourcing agreement for critical or important functions to set out the reporting obligations of the service provider to the institution or payment institution, including the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the critical or important function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements and, as appropriate, the obligations to submit reports of the internal audit function of the service provider.	<p>There is a requirement in the MiFID II Delegated Regulation and the EBA Guidelines for outsourcing firms to ensure that the service provider communicates any development that may have a material impact on its ability to effectively carry out the critical or important function and comply with applicable laws and regulatory requirements. The EBA Guidelines contain an additional obligation to ensure the reporting of reports of the internal audit function of the service provider.</p> <p>The EBA Guidelines explain, in reply to Consultation Paper responses, that institutions and payment institutions should assess whether third-party certification and reports are adequate and sufficient to comply with their regulatory obligations and should not rely solely on these reports over time.</p> <p>As noted above, reference in the EBA Guidelines to the internal audit function reporting is likely to be represented in MiFID II Delegated Regulation Article 31(2)(i), requiring effective access to data related to the outsourced functions, as well as to the relevant business premises of the service provider, where necessary for the purpose of effective oversight in accordance with Article 31.</p>
<b>Obligation to take appropriate measures</b>	Under Article 31(2)(d) of MiFID II Delegated Regulation, the outsourcing firm must ensure that appropriate action is taken where it appears that the service provider may not be carrying out the functions effectively or in compliance with applicable laws and regulatory requirements.	<p>Paragraph 105 of the EBA Guidelines requires institutions to take appropriate measures if they identify shortcomings in the provision of the outsourced function. In particular, institutions and payment institutions should follow up on any indications that service providers may not be carrying out the outsourced critical or important function effectively or in compliance with applicable laws and regulatory requirements.</p> <p>Under the EBA Guidelines, if shortcomings are identified, institutions and payment institutions should take appropriate corrective or remedial measures. Such actions may include terminating the outsourcing agreement, with immediate effect, if necessary.</p>	The obligation on the outsourcing firm to take appropriate measures where the service provider is not carrying out its functions effectively or in compliance with applicable laws and regulatory requirements exists in both the MiFID II Delegated Regulation and the EBA Guidelines. However, the EBA Guidelines additionally specify that this may include action to terminate the agreement. Though this is not specified in MiFID II Delegated Regulation it will fall within the more general requirement in Article 31(2)(d) of MiFID II Delegated Regulation to take "appropriate action".
<b>Cooperation with competent authorities</b>	Under Article 31(2)(h) of the MiFID II Delegated Regulation, the outsourcing firm should ensure that the service provider cooperates with the competent authorities of the outsourcing firm	Similarly, Paragraph 75(n) of the EBA Guidelines create an obligation on the outsourcing firm to set out in the outsourcing agreement the obligation of the service provider to cooperate with	The only distinction between the provisions in the MiFID II Delegated Regulation and the EBA Guidelines is the additional reference in the EBA Guidelines to resolution authorities. This creates

Topic	MiFID II Delegated Regulation	EBA Guidelines	Comparison
	in connection with the outsourced functions.	the competent authorities and resolution authorities of the institution or payment institution, including other persons appointed by them.	the requirement, in the context of the UK, for the service provider to cooperate with the BOE.
<b>Access to data</b>	Article 31(2)(i) of the MiFID II Delegated Regulation requires the outsourcing firm to ensure that the outsourcing firm, its auditors, and the relevant competent authorities, have effective access to data related to the outsourced functions, as well as to the relevant business premises of the service provider, where necessary for the purpose of effective oversight in accordance with Article 31, and the competent authorities are able to exercise those rights of access.	The equivalent EBA Guidelines provision is at Paragraph 36. This states that the institutions', payment institutions' and competent authorities', including resolution authorities, right to inspections and access to information, accounts and premises should be ensured within the written outsourcing agreement. The right to audit is key to providing the appropriate assurance that at least critical or important outsourced functions, as well as functions that may become critical or important in the future, are provided as contractually agreed and in line with regulatory requirements. However, audit and access rights for competent authorities need to be ensured for all outsourcing arrangements to ensure that institutions can be effectively supervised.	The requirement for the outsourcing firm to ensure its access to necessary data and the business premises, for itself and the relevant competent authority, is therefore the same in both the MiFID II Delegated Regulation and the EBA Guidelines. As above, the EBA Guidelines make reference to resolution authorities. This creates the requirement, in the context of the UK, for the service provider to cooperate with the BOE.
<b>Protection of confidential information</b>	Article 31(2)(j) of the MiFID II Delegated Regulation requires the outsourcing firm to ensure the service provider protects any confidential information relating to the investment firm and its clients.	This requirement is found in Paragraph 37 of the EBA Guidelines, stating that institutions and payment institutions must ensure that personal data are adequately protected and kept confidential.	The provisions of the MiFID II Delegated Regulation and the EBA Guidelines are aligned.
<b>Contingency planning</b>	The MiFID II Delegated Regulation requires the outsourcing firm to ensure that the outsourcing firm and the service provider have established, implemented and maintained a contingency plan for disaster recovery and periodic testing of backup facilities, where that is necessary having regard to the function, service or activity that has been outsourced.	Paragraph 75(l) of the EBA Guidelines state that the outsourcing agreement must set out requirements to implement and test business contingency plans.  In its response to replies to the Consultation Paper, the EBA clarifies that business continuity plans should take into account the possibility that the quality of the provision of the outsourced critical or important function will deteriorate to an unacceptable level or fail. Such plans should also take into account the potential impact of the insolvency, or other failures, of service providers and, where relevant, political risks in the service provider's jurisdiction.	Though both the MiFID II Delegated Regulation and the EBA Guidelines require the maintenance and testing of business contingency plans, the MiFID II Delegated Regulation also specifies that this should include the periodic testing of backup facilities. This may be considered to be implicit in the EBA Guidelines.
<b>Business continuity</b>	The MiFID II Delegated Regulation requires the outsourcing firm to ensure that the continuity and quality of the outsourced functions or services are maintained in the event of termination of the outsourcing either by transferring the outsourced functions or services to another third party or by performing them itself.	The same requirement is found in Paragraph 107 of the EBA Guidelines, which states that institutions and payment institutions should ensure that they are able to exit outsourcing arrangements without undue disruption to their business activities, without limiting their compliance with regulatory requirements and without any detriment to the continuity and	Therefore, though the requirements as to business continuity arrangements are aligned with the MiFID II Delegated Regulation as in the EBA Guidelines, the EBA Guidelines contain the additional specific requirements that the outsourcing firm develop exit plans containing analyses and cost/impact reports to achieve this.

Topic	MiFID II Delegated Regulation	EBA Guidelines	Comparison
		<p>quality of its provision of services to clients.</p> <p>The Guidelines state that in order to achieve this objective, the institution or payment institution should:</p> <ul style="list-style-type: none"> <li>a. develop and implement exit plans that are comprehensive, documented and, where appropriate, sufficiently tested (e.g., by carrying out an analysis of the potential costs, impacts, resources and timing implications of transferring an outsourced service to an alternative provider); and</li> <li>b. identify alternative solutions and develop transition plans to enable the institution or payment institution to remove outsourced functions and data from the service provider, and transfer them to alternative providers or back to the institution or payment institution, or to take other measures that ensure the continuous provision of the critical or important function or business activity in a controlled and sufficiently tested manner, taking into account the challenges that may arise because of the location of data and taking the necessary measures to ensure business continuity during the transition phase.</li> </ul>	
<b>Outsourcing agreements</b>	<p>Article 31(3) of the MiFID II Delegated Regulation states that the respective rights and obligations of the outsourcing firm and of the service provider must be clearly allocated and set out in a written agreement. In particular, the outsourcing firm shall keep its instruction and termination rights, its rights of information, and its right to inspections and access to books and premises. The agreement should ensure that outsourcing by the service provider only takes place with the consent, in writing, of the outsourcing firm.</p>	<p>Paragraph 74 of the EBA Guidelines sets out that the rights and obligations of the institution, the payment institution and the service provider should be clearly allocated and set out in a written agreement.</p> <p>Paragraph 75 of the EBA Guidelines sets out what the written agreement should include:</p> <ul style="list-style-type: none"> <li>a. a clear description of the outsourced function to be provided;</li> <li>b. the start date and end date, where applicable, of the agreement and the notice periods for the service provider and the</li> </ul>	<p>Though it may appear that the EBA Guidelines contain considerably more stringent requirements as to the contents of an outsourcing agreement, each of the items in this list features as a requirement on outsourcing firms to ensure from service providers in Article 31(2) of the MiFID II Delegated Regulation, as noted above.</p>



Topic	MiFID II Delegated Regulation	EBA Guidelines	Comparison
		<p>institution or the payment institution;</p> <ul style="list-style-type: none"> <li>c. the governing law of the agreement;</li> <li>d. the parties' financial obligations;</li> <li>e. whether the sub-outsourcing of a critical or important function, or material parts thereof, is permitted, and if so, the conditions that the sub-outsourcing is subject to;</li> <li>f. the location(s) (i.e., regions or counties) where the critical or important function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the institution or payment institution if the service provider proposes to change the location(s);</li> <li>g. where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data;</li> <li>h. the right of the institution or payment institution to monitor the service provider's performance on an ongoing basis;</li> <li>i. the agreed service levels, which should include precise quantitative and qualitative performance targets for the outsourced function to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met;</li> <li>j. the reporting obligations of the service provider to the institution or payment institution, including the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the critical or important function in line with the agreed service levels and in compliance with applicable laws and</li> </ul>	

Topic	MiFID II Delegated Regulation	EBA Guidelines	Comparison
		<p>regulatory requirements and, as appropriate, the obligations to submit reports of the internal audit function of the service provider;</p> <ul style="list-style-type: none"> <li>k. whether the service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;</li> <li>l. the requirements to implement and test business contingency plans;</li> <li>m. provisions to ensure that the data that are owned by the institution or payment institution can be accessed in the case of the insolvency, resolution or discontinuation of the business operations of the service provider;</li> <li>n. the obligation of the service provider to cooperate with the competent authorities and resolution authorities or payment institution, including other persons appointed by them;</li> <li>o. for institutions, a clear reference to the national resolution authority's powers, especially to Articles 68 and 71 of the BRRD, and in particular a description of the "substantive obligations" of the contract in the sense of Article 68 of the BRRD;</li> <li>p. the unrestricted right of institutions, payment institutions and competent authorities to inspect and audit the service provider with regard to, in particular, the critical or important outsourced function; and</li> <li>q. termination rights.</li> </ul>	
<b>Intra-group outsourcing</b>	Article 31(4) of the MiFID II Delegated Regulation provides that where the outsourcing firm and the service provider are members of the same group, the investment firm may, for the purposes of complying with Article 31 and Article 32, take into account the extent to which the firm controls the service provider or has the ability to influence its actions.	This provision for taking into account the level of control a group member may have is also found in Paragraph 116 of the EBA Guidelines, which states that institutions should consider whether the service provider is a subsidiary or a parent undertaking of the institution, is included in the scope of accounting consolidation or is a member of or owned by institutions that are members of an	Therefore, in both the MiFID II Delegated Regulation and the EBA Guidelines, the extent to which the outsourcing firm controls the service provider is an applicable consideration for the purposes of compliance with the provisions in an intra-group context.

Topic	MiFID II Delegated Regulation	EBA Guidelines	Comparison
		IPS and, if so, the extent to which the institution controls it or has the ability to influence its actions in line with Section 2 of the EBA Guidelines.	
<b>Obligations to the competent authority</b>	Under Article 31(5) of the MiFID II Delegated Regulation, the outsourcing firm should make available on request to the competent authority all information necessary to enable the authority to supervise the compliance of the performer of the outsourced functions with the requirements of MiFID II and its implementing measures.	Under Paragraph 57 of the EBA Guidelines, institutions and payment institutions should, upon request, make available to the competent authority all information necessary to enable the competent authority to execute the effective supervision of the institution or the payment institution, including, where required, a copy of the outsourcing agreement.	Though the EBA Guidelines specify in particular that the outsourcing firm should make available a copy of the outsourcing agreement, this is implicit in the MiFID II Delegated Regulation requirement to make available "all information necessary".
<b>Third country outsourcing</b>	<p>Under Article 32 of the MiFID II Delegated Regulation, where an outsourcing firm outsources functions related to the investment service of portfolio management provided to clients to a service provider located in a third country, that outsourcing firm ensures that the following conditions are satisfied:</p> <ul style="list-style-type: none"> <li>a. the service provider is authorised or registered in its home country to provide that service and is effectively supervised by a competent authority in that third country; and</li> <li>b. there is an appropriate cooperation agreement between the competent authority of the investment firm and the supervisory authority of the service provider.</li> </ul> <p>Further, the cooperation agreement referred to above shall ensure that the competent authorities are able, at least, to:</p> <ul style="list-style-type: none"> <li>a) obtain, upon request, the information necessary to carry out their supervisory tasks pursuant to the CRD IV, Capital Requirements Regulation 2013, Payment Services Directive and the E-Money Directive;</li> <li>b) obtain access to any data, documents, premises or personnel in the third country that are relevant for the performance of their supervisory powers;</li> <li>c) receive, as soon as possible, information from the supervisory authority in the third</li> </ul>	<p>The relevant provision in the EBA Guidelines is in Paragraph 63, which provides for outsourcing to a service provider in a third country only if:</p> <ul style="list-style-type: none"> <li>a. the service provider is authorised or registered to provide that banking activity or payment service in the third country and is supervised by a relevant competent authority in that third country (referred to as a "supervisory authority");</li> <li>b. there is an appropriate cooperation agreement, e.g., in the form of a memorandum of understanding or college agreement, between the competent authorities responsible for the supervision of the institution and the supervisory authorities responsible for the supervision of the service provider; and</li> <li>c. the cooperation agreement referred to in point (b) should ensure that the competent authorities are able, at least, to: <ul style="list-style-type: none"> <li>i. obtain, upon request, the information necessary to carry out their supervisory tasks pursuant to the CRD IV, Capital Requirements Regulation 2013, Payment Services Directive and the E-Money Directive;</li> <li>ii. obtain appropriate access to any data,</li> </ul> </li> </ul>	<p>It should be noted that the EBA Guidelines refer to "banking activities and payment services" whilst the delegated regulation refers to portfolio management. The EBA Guidelines state that this is "in line with the approach for investment services under Article 32 of the MiFID II Delegated Regulation, which requires such a cooperation agreement in the case of outsourcing functions of portfolio management; it ensures that the rights and responsibilities of the competent authority and the supervisory authority would be set out in writing".</p> <p>There is no direct reference in the EBA guidelines to portfolio management, only to banking activities and payment services. However, the provisions are identical for both.</p>

Topic	MiFID II Delegated Regulation	EBA Guidelines	Comparison
	<p>country for investigating apparent breaches of the requirements of the CRD IV, Capital Requirements Regulation 2013, Payment Services Directive and the E-Money Directive; and</p> <p>d) cooperate with the relevant supervisory authorities in the third country on enforcement in the case of a breach of the applicable regulatory requirements and national law in the Member State. Cooperation should include, but not necessarily be limited to, receiving information on potential breaches of the applicable regulatory requirements from the supervisory authorities in the third country as soon as is practicable.</p>	<p>documents, premises or personnel in the third country that are relevant for the performance of their supervisory powers;</p> <p>iii. receive, as soon as possible, information from the supervisory authority in the third country for investigating apparent breaches of the requirements of the CRD IV, Capital Requirements Regulation 2013, the Payment Services Directive and the E-Money Directive; and</p> <p>iv. cooperate with the relevant supervisory authorities in the third country on enforcement in the case of a breach of the applicable regulatory requirements and national law in the Member State. Cooperation should include, but not necessarily be limited to, receiving information on potential breaches of the applicable regulatory requirements from the supervisory authorities in the third country as soon as is practicable.</p>	

# ABOUT THE AUTHORS

---

## About AFME

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues.

We represent the leading global and European banks and other significant capital market players.

We advocate for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society.

We aim to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work.

## About Latham & Watkins

Latham & Watkins delivers innovative solutions to complex legal and business challenges around the world. From a global platform, our lawyers advise clients on market-shaping transactions, high-stakes litigation and trials, and sophisticated regulatory matters. Latham is one of the world's largest providers of pro bono services, steadfastly supports initiatives designed to advance diversity within the firm and the legal profession, and is committed to exploring and promoting environmental sustainability.

Latham & Watkins has established a leading financial regulatory practice in Europe. Led by a number of the region's most distinguished practitioners, the diverse and commercially-focused team advises a broad array of prominent financial institutions, including investment managers, banks, infrastructure providers, and fintech firms. The team has developed a particular reputation for the commerciality and practicality of its approach and advice.

## About Matheson

Matheson is the law firm of choice for internationally focused companies and financial institutions doing business in and from Ireland. Our standards of client care have been built on the implementation of a clear client-focused strategy; a commitment to legal excellence; and the calibre of our legal and business services professionals. Our core values of partnership, respect, innovation, diversity and entrepreneurship characterise our collective dynamic as a firm, and push us to achieve the highest standards as legal professionals and advisers to our clients.

Matheson's expertise is spread across more than 30 practice groups and we work collaboratively across all areas, reinforcing a client first ethos among our people, and our broad and interconnected spread of industry and sectoral expertise allows us to provide the full range of legal advice and services to our clients. Our Financial Institutions Group unites lawyers with extensive industry experience, corporate transactional experience and regulatory knowledge who are solely focused on financial institutions. We continually look to use the breadth and depth of this experience to benefit our clients.

## About BSP

BSP is an independent full-service law firm based in Luxembourg.

We are committed to providing the very best legal services to our domestic and international clients in all aspects of Luxembourg business law.

Talented and multilingual, our teams of lawyers work side by side with our clients to help them reach their objectives and support them with tailor-made legal advice, creating in the process professional relationships based on mutual trust and respect.

Our lawyers have developed particular expertise in banking and finance, capital markets, corporate law, dispute resolution, employment law, investment funds, intellectual property, private wealth, real estate and tax. In these practice areas, as in others, our know-how, our ability to work in cross-practice teams and to swiftly adapt to new laws and regulations allow us to provide to our clients timely and integrated legal assistance vital to the success of their business.

Building on the synergy of our different professional experiences and the richness of our diverse cultural background, we stand ready to meet our clients' legal needs, no matter how challenging they are.



# CONTACTS FOR FURTHER ADVICE

---

## AFME

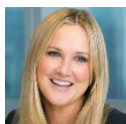


**Richard Middleton**  
[richard.middleton@afme.eu](mailto:richard.middleton@afme.eu)



**Louise Rodger**  
[louise.rodger@afme.eu](mailto:louise.rodger@afme.eu)

## UK



**Nicola Higgs**  
[nicola.higgs@lw.com](mailto:nicola.higgs@lw.com)



**Fiona Maclean**  
[fiona.maclean@lw.com](mailto:fiona.maclean@lw.com)



**Andrew Moyle**  
[andrew.moyle@lw.com](mailto:andrew.moyle@lw.com)



**Anne Mainwaring**  
[anne.mainwaring@lw.com](mailto:anne.mainwaring@lw.com)



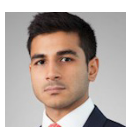
**Jagveen Tyndall**  
[jagveen.tyndall@lw.com](mailto:jagveen.tyndall@lw.com)



**Oscar Bjartell**  
[oscar.bjartell@lw.com](mailto:oscar.bjartell@lw.com)



**Sean Wells**  
[sean.wells@lw.com](mailto:sean.wells@lw.com)



**Sidhartha Lal**  
[sidhartha.lal@lw.com](mailto:sidhartha.lal@lw.com)

## SPAIN

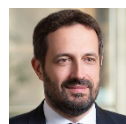


**Ignacio Gómez-Sancha**  
[ignacio.gomez-sancha@lw.com](mailto:ignacio.gomez-sancha@lw.com)



**Rafael Martínez-Echevarría**  
[rafael.martinez-echevarria@lw.com](mailto:rafael.martinez-echevarria@lw.com)

## FRANCE



**Jean-Luc Juhan**  
[jean-luc.juhan@lw.com](mailto:jean-luc.juhan@lw.com)



**Ornella Capillon**  
[ornella.capillon@lw.com](mailto:ornella.capillon@lw.com)



**Léa Margono**  
[lea.margono@lw.com](mailto:lea.margono@lw.com)

## GERMANY



**Markus Krüger**  
[markus.krueger@lw.com](mailto:markus.krueger@lw.com)



**Axel Schiemann**  
[axel.schiemann@lw.com](mailto:axel.schiemann@lw.com)



**Thies Deike**  
[thies.deike@lw.com](mailto:thies.deike@lw.com)



**Max Von Cube**  
[max.voncube@lw.com](mailto:max.voncube@lw.com)

## ITALY



**Isabella Porchia**  
[isabella.porchia@lw.com](mailto:isabella.porchia@lw.com)



**Marco Bonasso**  
[marco.bonasso@lw.com](mailto:marco.bonasso@lw.com)



**Lorenzo Rovelli**  
[lorenzo.rovelli@lw.com](mailto:lorenzo.rovelli@lw.com)



**Marta Carini**  
[marta.carini@lw.com](mailto:marta.carini@lw.com)

## IRELAND



**Joe Beashel**  
[joe.beashel@matheson.com](mailto:joe.beashel@matheson.com)



**Louise Dobbyn**  
[louise.dobbyn@matheson.com](mailto:louise.dobbyn@matheson.com)

## LUXEMBOURG



**Evelyn Maher**  
[emaher@bsp.lu](mailto:emaher@bsp.lu)



**Nuala Doyle**  
[ndoyle@bsp.lu](mailto:ndoyle@bsp.lu)



**Elzbieta Tumko**  
[etumko@bsp.lu](mailto:etumko@bsp.lu)



**Christoforos Soteriou**  
[csoteriou@bsp.lu](mailto:csoteriou@bsp.lu)



**Deniz Günes Türktas**  
[dgunesturktas@bsp.lu](mailto:dgunesturktas@bsp.lu)



**Marta Gajos**  
[mgajos@bsp.lu](mailto:mgajos@bsp.lu)