FINANCIAL REGULATION
TECHNOLOGY

Outsourcing: Risk Assessments and Due Diligence - Key points from the Central Bank's draft cross-industry guidance

April 2021

This briefing focuses on aspects of the Central Bank's recent draft cross-industry guidance on outsourcing regarding outsourcing risk assessments and due diligence.

INTRODUCTION

Outsourcing remains very high on the supervisory agenda of the Central Bank (**CBI**), with the recent launch of a consultation on draft cross-industry guidance for all regulated firms (the **CBI Guidance**). Following on from our recent overview of the CBI Guidance and our detailed briefing on its key Governance and Monitoring aspects, this briefing focuses on the aspects relating to the conduct of outsourcing **risk assessments** and the Central Bank's expectations in relation to carrying out **due diligence** on outsourced service providers (**OSPs**).

FOCUS ON OUTSOURCING

In February 2021, the CBI published CP138 - Consultation on Cross-Industry Guidance on Outsourcing (**CP138**) together with its draft CBI Guidance.

Outsourcing is a key focus of the CBI's supervisory agenda and, as drafted, the CBI Guidance is applicable to all regulated firms that outsource services and/or functions (see our recent overview: Outsourcing: Central Bank consults on draft cross-industry guidance for regulated firms for further information).

Two of the key issues that the CBI Guidance focuses on are:

- developing a strong risk management framework (**Risk Framework**) and comprehensive risk assessments to enable regulated firms to appropriately monitor, manage and mitigate outsourcing risks; and
- the CBI's expectations regarding the due diligence that regulated firms should carry out on OSPs.

We explore these issues in more detail in this briefing.

RISK ASSESSMENT REQUIREMENTS

Part B, Section 5 of the CBI Guidance sets out the CBI's expectations surrounding effective monitoring, management and mitigation of the risks associated with outsourcing. This requires regulated firms to develop and implement a robust outsourcing Risk Framework and to ensure that risks inherent in all outsourced functions, activities, processes and systems are appropriately identified, monitored and managed.

When developing the Risk Framework and conducting risk assessments, the CBI expects a regulated firm to:

- ensure that its Risk Framework considers any outsourcing arrangements and that outsourcing risks are identified in the regulated firm's overarching risk register;
- conduct comprehensive risk assessments prior to entering into any proposed outsourcing arrangement;
- ensure that outsourcing risk assessments are tailored to take account of specific risks (e.g. sensitive data risks, offshoring risks, business continuity risks, sub-outsourcing risks, step-in risks and legal, regulatory and reputational risks);
- consider and document the controls to be put in place to minimise exposure to any identified outsourcing risks and ensure that these controls are enshrined in the relevant outsourcing contracts and/or service level agreements (**SLAs**), as appropriate;
- regularly review its outsourcing arrangements, with particular focus on critical or important arrangements (such reviews should consider whether the nature, scale or complexity of the outsourced function or the risks associated with it have changed since its inception or last review, whether this impacts its assessment of the criticality or importance of that outsourced function, and if there have been any other changes in the regulated firm's exposure to concentration risk (whether via its OSPs or due to

new or amended sub-outsourcing arrangements)); and

- review and refresh risk assessments on a periodic basis to ensure that they continue to accurately reflect the regulated firm's business (including for example, its operating environment, and applicable legal and regulatory requirements), to ensure that those assessments continue to reflect the current risks to which the regulated firm is exposed, and to take account of any material changes to the regulated firm's OSPs.

Sub-Outsourcing Risk

The CBI notes that:

- sub-outsourcing can complicate the effective management of outsourcing risk, as the parties involved can be spread across different physical and geographical locations;
- regulated firms may also develop dependencies on a sub-contracted provider without being aware of those dependencies (if they are not notified of the planned sub-outsourcing); and
- concentrations may also develop in respect of sub-outsourced providers, which the regulated firm does not have sight of (*concentration risk is discussed in more detail below*).

To manage the risks associated with sub-outsourcing effectively, the CBI expects a regulated firm to:

- determine its appetite for sub-outsourcing as part of its outsourcing policy;
- manage the associated risks via specific provisions in its contractual arrangements/SLAs;
- treat outsourcing risk (including sub-outsourcing risk) arising from intragroup arrangements in the same way as it treats the equivalent risk arising from arrangements with external third party OSPs; and
- ensure that, at a minimum, the OSP oversees and manages the activities of the sub-OSP to ensure that all services are fulfilled in line with the original outsourcing contract/SLA.

Sensitive Data Risk and Data Security

Sensitive Data Risk

To prevent data breaches or unauthorised disclosure of customer, employee or commercially sensitive data, the CBI expects regulated firms to implement effective measures for the appropriate storage, management, retention and destruction of this data.

Measures to effectively manage risks relating to the potential loss, alteration, destruction or unauthorised disclosure of a regulated firm's sensitive data should include:

- implementing appropriate measures to secure and protect that data and including these measures in the firm's outsourcing policy and SLAs;
- as good practice, having a documented data management strategy that addresses the range of risks which can arise in the context of outsourcing, including those relating to data transmission and storage;
- ensuring compliance with the General Data Protection Regulation (**GDPR**) and other applicable data protection legislation applying to the regulated firm's operations; and
- designing a comprehensive security architecture, the implementation of which may fall to both the regulated firm and related OSPs.

Data Security – Availability and Integrity

The CBI acknowledges that the requirement to ensure the availability and integrity of data drives the requirements for secure transmission, storage and backup arrangements.

The CBI expects regulated firms to ensure implementation of appropriately designed and operationally effective controls, whether implemented by the regulated firm or an OSP on the regulated firm's behalf.

These controls should include a range of measures including configuration management, encryption and key management, incident detection, access/activity logging and loss recovery.

Concentration Risk

In an outsourcing context, concentration risk is the probability of loss arising from a lack of diversification of OSPs.

The CBI notes that concentration risk may arise:

- at an individual firm level, where the regulated firm relies on a single or small number of OSPs (including intra-group OSPs) to provide critical or important activities; or
- at a sectoral level, where multiple regulated firms share a common dependency which cannot be easily substituted (i.e. where a limited number of OSPs are available (which is an emerging issue in the context of specialist services like cloud services).

Concentration risk can also arise indirectly from any sub-outsourcing undertaken by the OSP.

To manage and mitigate against these risks, the CBI expects a regulated firm to:

- regularly take adequate steps to assess its overall reliance on OSPs (and sub-contractors) and manage concentration risks;
- ensure its Risk Framework includes the approach for the identification, management and reporting of concentration risk;
- ensure its ability to negotiate and secure appropriate arrangements is not restricted, even where there is a relatively small pool of OSPs to choose from;
- include terms in the contract between the regulated firm and the OSP requiring the regulated firm's consent to any sub-outsourcing arrangement; and
- evaluate the concentration risk in the risk assessments and due diligence review when outsourcing critical or important functions.

Offshoring Risk and Potential Constraints

The CBI notes that outsourcing to offshore jurisdictions poses specific risks arising from the physical distance between the OSP and the regulated firm. This is problematic for both the regulated firm and the CBI from a supervisory/visibility perspective and may impede the CBI's ability to effectively oversee and supervise the offshore arrangement(s).

When outsourcing to offshore jurisdictions, the CBI expects a regulated firm to:

- evaluate the particular risks associated with countries to which it is planning to outsource activities;
- pay attention to the "country risk" in its risk assessment and in assessing the country risk, take into account the country's regulatory environment, legal risk, political and physical climate risk, any cultural or language issues and employment conditions; and
- ensure there are minimum standards in place at the OSP in respect of risk appetite and that these are aligned with the regulated firm's risk management expectations.

The CBI expects, where potential constraints to outsourcing might arise, that regulated firms will inform the CBI before committing to any offshoring arrangement of critical/important functions. The CBI also expects regulated firms to assess the criticality or importance of proposed outsourcing at an early stage so they can discuss the

risks associated with the offshoring with the CBI.

DUE DILIGENCE REQUIREMENTS

Part B, Section 6 of the CBI Guidance sets out the CBI's expectation that appropriate and proportionate due diligence reviews will be conducted in respect of all prospective OSPs or intragroup providers before entering into any arrangements.

It is important to note that the CBI Guidance requires regulated firms to ensure that the OSP has the capabilities, and the appropriate authorisation, where required, to perform the **critical or important function(s)** in a reliable and professional manner for the term of the contract/SLA.

The CBI expects that when conducting the initial due diligence review in respect of OSPs, a regulated firm will consider at least the following:

- the nature and scale of the OSP (including its business model, complexity, financial situation/ performance, business reputation, ownership and group structure);
- the long-term relationships with OSPs that have already been assessed and any services already performed by the OSP for the regulated firm;
- whether the OSP is a parent undertaking or subsidiary of the regulated firm (i.e. is it an intra-group arrangement?);
- compliance with the GDPR and other applicable data protection laws and regulatory requirements;
- whether the OSP is authorised by a regulatory authority to provide the service and whether or not the OSP is supervised by competent authorities;
- whether the OSP is well-positioned to align with innovation in the relevant sector;
- potential conflicts of interest (particularly in the case of intra-group arrangements); and
- the effectiveness of risk management and internal controls, including IT and cybersecurity, to protect the data in accordance with the regulated firm's data management strategy (as described in Part B, Section 5.2 of the CBI Guidance).

The CBI Guidance also sets out an additional list of criteria which the CBI expects the due diligence carried out by a regulated firm to consider. This includes the potential exposure to concentration risk, the managerial skills of the regulated firm to oversee the OSP, the skills within the OSP, insurance cover of the OSP, incident reporting and management programmes, and the OSP's track record.

Values and Ethical Behaviour – Regulatory Expectations

In line with EBA Guidelines on Outsourcing and general good practices, the CBI expects regulated firms to take adequate steps to ensure that OSPs act in a manner consistent with the values and code of conduct of the regulated firm. This includes taking measures to ensure they are satisfied that OSPs located in third countries (and if applicable their sub-contractors) act in an ethical and socially responsible manner and adhere to international standards on human rights.

Frequency of Due Diligence Review Performance

The CBI expects that a regulated firm will conduct an initial wide-ranging due diligence review of the OSP's operational and financial capacity.

For key OSPs that provide critical or important services, a brief review of the financial health should be conducted each year. Otherwise, reviews should be carried out periodically over the lifecycle of the contract/SLA.

Prior to the expiry of key OSP contracts/ SLAs, regulated firms should undertake a review in order to inform the decision of whether or not to renew the agreement.

DETAILED FOLLOW-UP BRIEFINGS

Our penultimate briefing in our series of detailed follow-up briefings on the CBI Guidance will focus on contractual requirements applicable to outsourcing arrangements/SLAs and will set out practical steps that regulated firms can take in advance of the expected publication of the final CBI Guidelines later this year.

KEY CONTACTS

Orla O'Connor
Partner, Chair of the Firm
+353 1 920 1181
orla.oconnor@arthurcox.com

Robert Cain
Partner
+353 1 920 1050
robert.cain@arthurcox.com

Sarah Thompson
Partner
+44 28 9026 5894
sarah.thompson@arthurcox.com

Maedhbh Clancy
Of Counsel
+353 1 920 1225
maedhbh.clancy@arthurcox.com

Ian Duffy
Associate
+353 1 920 2035
ian.duffy@arthurcox.com

Kim O'Dowd
Associate
+353 1 920 1277
kim.odowd@arthurcox.com