Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Schedule 1 – Draft Cross-Industry Guidance on Outsourcing

February 2021

1 Contents

Note:

This Draft Cross-Industry Guidance on Outsourcing should be read in conjunction with Consultation Paper 138 – February 2021.

Part A - Introduction

1. Background

The Strategic Plan of the Central Bank of Ireland ('the Central Bank') sets out its Mission, Vision and Mandate. The Mission of the Central Bank is to serve the public interest by safeguarding monetary and financial stability and by working to ensure that the financial system operates in the best interests of consumers and the wider economy. In discharging its functions and exercising its powers, the Central Bank's mandate incorporates a number of statutory objectives. The 'Cross Industry Guidance on Outsourcing' ('the Guidance') set out herein, is published in the context of a number of these objectives, particularly[1]:

- Contributing to the stability of the financial system;
- The proper and effective regulation of financial service providers and markets, while ensuring that the best interests of consumers of financial services are protected; and
- The resolution of financial difficulties in credit institutions, certain investment firms and credit unions.

The Central Bank has also prioritised five strategic themes, which have been identified as being critical to the successful delivery of its mandate. The themes of 'Strengthening Resilience' so that the financial system is better able to withstand external shocks and future crises; and 'Strengthening Consumer Protection' so that the best interests of consumers are protected and confidence and trust in the financial system is enhanced through effective regulation of firms and markets, are of particular relevance to the publication of this Guidance.

The Central Bank is strongly focused on outsourcing due to its increasing prevalence across the financial services sector and its potential, if not effectively managed, to threaten the operational resilience of financial service providers regulated by the Central Bank ('regulated firms') and the Irish financial system. This would undermine the attainment of some of the key statutory objectives, which the Central Bank is mandated to achieve. Robust and effective outsourcing risk management within regulated firms supports the financial and operational resilience of these firms and consequently facilitates financial stability aims.

In recent years, the Central Bank has undertaken a significant programme of work in relation to outsourcing[2] and the management by regulated firms of risks presented by outsourcing arrangements. This programme of work has included:

[1] For further information, please refer to the Central Bank's Strategic Plan 2019 – 2021, which can be found here: https://www.centralbank.ie/publication/corporate-reports/strategic-plan.

[2] The general term 'outsourcing' is used in this paper in place of other terms, which may be used in specific sectors e.g. 'delegation'.

- A "Cross Sector Survey of Regulated Firms' Outsourcing Activity", which issued to 185 regulated firms in 2017;
- The publication of the discussion paper 'Outsourcing – Findings and Issues for Discussion'[3] in November 2018;
- The hosting of an industry Outsourcing Conference in April 2019; and
- Ongoing outsourcing related supervisory engagements, including risk assessments, inspections and thematic reviews.

During the conduct of this programme of work, the European Banking Authority ('the EBA') updated the 2006 guidelines on outsourcing that were issued by the Committee of European Banking Supervisors (CEBS). The updated guidelines on outsourcing, EBA/GL/2019/02, were published in February 2019 and came into force in September 2019. These guidelines also incorporated the EBA's 2017 recommendations on outsourcing to cloud service providers (CSPs). The aim of the EBA Guidelines is to "establish a more harmonised framework for all financial institutions that are within the scope of the EBA's mandate, namely credit institutions and investment firms subject to the Capital Requirements Directive (CRD), as well as payment and electronic money institutions"[4].

2019 and 2020 also saw the publication of the following:

- EBA Guidelines on ICT and security risk management (EBA ICT Guidelines);
- European Insurance and Occupational Pensions Authority (EIOPA) Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002);
- International Organization of Securities Commissions (IOSCO) Principles on Outsourcing – Consultation Report (Finalisation Q2 - 2021); and
- European Securities and Markets Authority ESMA 50-157-2403 Guidelines on Outsourcing to Cloud Service Providers (December 2020).
- EIOPA Guidelines on ICT Security and Governance BoS-20/600

The Central Bank views the management of outsourcing risk as key from both a Prudential and Conduct perspective. Boards and senior management must be cognisant of the fact that when entering into outsourcing arrangements they are creating a dependency on a third party, which has the potential to influence the operational resilience of their firm. The COVID–19 pandemic in 2020

[3] https://www.centralbank.ie/docs/default-source/publications/discussion-papers/discussion-paper-8/discussion-paper-8---outsourcing-findings-and-issues-for-discussion.pdf?sfvrsn=12
[4] https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf

has emphasised the need for resilience in the operation of outsourcing arrangements and reinforces the need for effective governance and oversight of the arrangements.

Regulated firms are expected to have effective governance, risk management and business continuity processes in place in relation to outsourcing, to mitigate potential risks of financial instability and consumer detriment. The guidance set out herein is designed to assist regulated firms in developing their outsourcing risk management frameworks to effectively identify, monitor and manage their outsourcing risks. The Central Bank's supervisory framework will apply a risk-based approach to assess the effectiveness of regulated firms governance and management of outsourcing arrangements and their adherence to and implementation of this Guidance.

Terms Commonly Used in the Guidance - Definitions

There are a number of terms and acronyms referring to aspects of outsourcing, which are used throughout this Guidance. The definitions for these terms are contained in Appendix 4 at the rear of this document.

2. Context

The nature of the financial services landscape is continually changing. Change is being influenced by many factors including customer/client preferences, regulatory concerns, the increased pace of technological innovation in the delivery of services, and changes in business models driven by cost, profitability and the need for increased flexibility and agility. Outsourcing is at the heart of much of this change and is increasingly being adopted as a key strategic tool to enable regulated firms to manage these changes. The Central Bank recognises the increasing reliance of many regulated firms on outsourced service providers (OSPs). This includes the use of both intragroup entities and third party OSPs, both regulated and unregulated, for the provision of activities and services considered central to the successful delivery of regulated firms' strategic objectives. Furthermore, given the continually changing landscape for the provision of financial services and the adaptation of regulated firms in responding to this change the Central Bank anticipates that there will be new structures and business models brought into being to deliver critical and important services. The Central Bank is already seeing some of these transformative capabilities emerging, which will be increasingly controlled by services providers who sit outside the traditional boundaries of the regulated financial services industry. This is leading to the creation of new service delivery models such as strategic partnering, cross-industry shared service centres and extensive sub-outsourcing, The development and use of these new models to deliver critical and important services or functions by regulated firms will be regarded as outsourcing and regulated firms will be expected to apply this Guidance.

The Central Bank also recognises the increasing role of technology reflected in the recent rapid growth in the number of Fintech (Financial Technology) and Regtech (Regulatory Technology) firms, and the use of cloud service providers (CSPs) by regulated firms. The increase in the outsourcing of core IT activities is a key area of focus for the Central Bank as it potentially raises the risks to the resilience of individual regulated firms, and consequently to both the domestic Irish financial system and the wider EU and Global markets in which such firms are operating. There is a need for additional technological input to the control and oversight of these outsourcing arrangements. Most importantly there is a need for management of regulated firms to understand the specific risks relating to the outsourcing of their critical or important services to CSPs. Therefore, the Guidance sets out specific expectations in the management of risks associated with outsourcing related to Information and Communications Technology (ICT) including those arising when outsourcing to the cloud, in addition to the broader measures that should be adopted for all critical or important outsourcing arrangements.

While the Central Bank acknowledges that outsourcing presents significant and wide ranging benefits to regulated firms, it also poses risks if not effectively managed.

The storage and management of business sensitive and/or customer confidential data by third parties, including CSPs, raises potential data security risks that must be addressed and appropriately managed to prevent vulnerabilities arising. It is imperative that regulated firms have knowledge of where their data is stored and how it is secured, to ensure appropriate risk management processes and controls, including data protection are in place.

Oversight of outsourcing can be complicated by the use of sub-outsourcing (also referred to as chain outsourcing), whereby the OSP transfers the performance of an outsourced function or service to another provider. Outsourcing chains can become long and complex, therefore, specific measures must be put in place to ensure that regulated firms are aware of and have appropriate governance and risk management arrangements in place in respect of sub-outsourcing. It is particularly important to ensure that sub-outsourcing does not impair regulated firm's visibility and a regulator's supervisibility of activities being performed

The Central Bank recognises that offshoring is a significant feature of outsourcing by some regulated firms in Ireland. Visibility and supervisibility risk is also one of the key concerns associated with offshoring, arising from the physical distance of the regulated firm from where the activity or service is being provided, which may be outside the EU with a different regulatory regime and no effective Memoranda of Understanding (MoUs) in place. Offshoring in such circumstances can challenge both a regulated firm's and the competent authority's ability to ensure effective oversight and supervision.

The increasing use of outsourcing arrangements also gives rise to growing concentration risk concerns. Concentration risk can arise at an individual firm level, whereby a firm has a dependency on a single or small number of firms for the provision of critical or important outsourced functions. It can also arise at a sectoral or cross-sectoral level where these dependencies are shared by multiple firms in a sector or across sectors. Concentration risk is of particular concern where it is determined that there are a limited number of providers of certain services, for example in the case of CSPs or other specialist service providers, that may be difficult to substitute. Such concentrations can also give rise to broader systemic concentration risk concerns if not appropriately managed. The Central Bank's research suggests that there is a significant degree of concentration risk in respect of the provision of particular outsourced critical or important services in the Irish financial services sector and that in many cases, regulated firms may not be aware of their exposure to concentration risk in their outsourcing arrangements. Consequently, the Guidance provides clarity regarding concentration risk and the Central Bank's expectations of regulated firms for the identification and management of this risk. In this regard, regulated firms should be aware that discussions are ongoing at EU and international levels regarding systemic concentration risk and the potential implications on financial stability, which could arise because of dependence on systemically significant unregulated third parties such as the dominant Cloud Service Providers. The outcome of these discussions could result in changes to the regulatory framework over time.

3. Purpose & Scope

The Guidance is being introduced to supplement existing sectoral legislation, regulations and guidelines on outsourcing, by setting out the Bank's expectations of good practice for the effective management of outsourcing risk. The Guidance does not purport to address in detail, every aspect of firms' legal and regulatory obligations as they pertain to outsourcing and should be read in conjunction with the relevant legislation, regulations as well as guidance and standards issued by the European Supervisory Authorities (ESAs), IOSCO Principles on Outsourcing, BIS Principles on Operational Risk and Resilience and further guidelines/guidance or bulletins issued by the Central Bank. Details of the relevant sectoral legislation, regulations, guidelines and guidance, in force at a point in time, are included in Appendix 1 of this Guidance.

The Guidance also reminds regulated firms of their obligations concerning compliance with existing and future legislation, regulations and guidelines relevant to their sector, in respect of the management of outsourcing risk. Further details regarding the legal status of the Guidance can be found in Section 5 below.

Furthermore, the purpose of the Guidance is to:

- Communicate the Central Bank's expectations with respect to the governance and management of outsourcing risk to the boards and senior management of regulated firms;
- Remind boards and senior management of regulated firms of their responsibilities when considering utilising outsourcing as part of their business model;
- Ensure that the boards and senior management of regulated firms take appropriate action to ensure that their outsourcing frameworks are well designed, operating effectively and are sufficiently robust to manage the associated risks.

The Guidance also refers to the Central Bank's adoption of the EBA Guidelines on Outsourcing Arrangements, the EBA ICT Guidelines, the EIOPA Guidelines of Systems of Governance and the EIOPA and ESMA Guidelines for outsourcing to cloud service providers, for regulated firms that are within the scope of those guidelines. This Cross-Industry Guidance confirms the Central Bank's expectation that such firms make every effort to comply with those guidelines.

Notwithstanding the scope and application of the EBA Guidelines and the EIOPA Guidelines, the Central Bank is of the view that the requirements set out therein, and in other draft guidelines currently the subject of consultation (detailed in section 1.1 above) align with and underpin the Central Bank's own supervisory expectations in relation to the governance and management of outsourcing risk. The Central Bank's Guidance (the Guidance) as set out in this document is therefore in keeping with the requirements set out in the EBA Guidelines and the EIOPA and ESMA Guidelines. The Guidance will apply in a proportionate manner, to all regulated firms and not just those covered by the scope of the EBA, EIOPA and ESMA Guidelines.

The Guidance sets out the Central Bank's expectations where certain provisions of the EBA Guidelines and the EIOPA guidelines allow for National Competent Authority discretions e.g. notification of outsourcing and maintenance and submission of outsourcing registers; (see sections 10.1. and 10.2 of the Guidance).

The Central Bank may update or amend the Guidance from time to time, as and when the need arises.

4. Application of the Guidance and Proportionality

The Central Bank deems this guidance relevant to any regulated firm, which utilises outsourcing as part of their business model. In adopting the Guidance setout herein, regulated firms should always have regard to the principle of proportionality, whereby the nature and extent of measures to be applied may be adapted and applied in a proportionate manner. In its consideration of proportionality, a regulated firm should have regard to the nature, scale and complexity of its

business and the degree to which it engages in outsourcing to implement its business model. The test for proportionality should always be underpinned by the regulated firm's outsourcing risk assessment and resulting controls. The extent of measures applied should also be informed by the regulated firm's assessment of whether the outsourced service or activity is deemed critical or important (as set out in section 2.1 below). For the purpose of this Guidance, it is intended that the measures set out are to be applied in respect of a regulated firm's critical or important outsourcing arrangements, except where it is highlighted that the requirements should take account of all outsourcing arrangements. However, regulated firms should determine where it might be prudent to apply the measures to non-critical or less important arrangements in line with their own risk assessment. Regulated firms may also wish to consider the application of the Guidance, or aspects of the Guidance, as a matter of good practice, to arrangements with other third party service providers or vendors, even where these arrangements do not fall within the definition of outsourcing.

Certain aspects of this Guidance may not be appropriate to all regulated firms, due to their nature, scale and complexity. The Central Bank acknowledges that it may not be appropriate for certain smaller, less complex regulated firms to adopt, in full, all measures set out in the Guidance. Regulated firms may decide to adopt different practices to those covered in this Guidance in ensuring compliance with the relevant sectoral legislation, regulation and guidelines (as detailed in Appendix 1) and in order to prudently manage any exposure to outsourcing risk. However, where they do so, the regulated firm is expected to be in a position to explain the reason, upon request, for proceeding as they have to the Central Bank. Regulated firms must be able to clearly evidence the rationale for their approach and that the approach has been considered and approved by the board or equivalent. All regulated firms must be able to demonstrate that they have appropriate measures in place to effectively govern and manage outsourcing risk and to ensure compliance with the sectoral legislation, regulations and guidance applicable to their business.

5. Status

This Guidance should be treated as a guide to good practice with regard to outsourcing. Regulated firms must always refer directly to the relevant sectoral legislation, regulations and guidance, in force, when ascertaining their statutory obligations – see Appendix 1 which contains a listing as of the date of publication of this Guidance.

This Guidance does not replace or override any legal and/or regulatory requirements. In the event of a discrepancy between the Guidance and the relevant sectoral legislation, the primacy of the legislation will apply. Where existing relevant sectoral legislation, regulations or guidance is less

prescriptive or is silent on certain matters, it is the Central Bank's expectation that regulated firms refer to the supervisory expectations set out in this Guidance, which is deemed good practice in the governance and management of outsourcing risk. If sectoral guidance is more prescriptive then it will take precedence over this Guidance.

The Guidance should not be construed as legal advice or legal interpretation. It is a matter for regulated firms to seek legal advice if they are unsure regarding their obligations as they apply to their particular set of circumstances.

Where lists or examples are included in the Guidance, such lists or examples are non-exhaustive. The lists are generally adapted from the EBA Guidelines on Outsourcing[5] and in some cases are supplemented by additional measures suggested by the Central Bank as a matter of good practice. The examples present some, but not the only ways, in which regulated firms might comply with their obligations. The Guidance does not take the place of a regulated firm performing its own assessment of the manner in which it shall comply with its statutory obligations or manage and mitigate its exposure to outsourcing risk. This may result in a regulated firm further supplementing the measures set out in the Guidance.

Part B -
Cross-Industry Guidance on Outsourcing Risk

1. Assessment of Criticality or Importance of activity/service to be outsourced

In order to manage outsourcing risk effectively it is necessary to determine the criticality or importance, to the regulated firm, of the function, service or activity ('the Function'), which is being outsourced. This should determine the risk management measures, which should be adopted to ensure resilience and continuity of operations. In conjunction with current legislation and or regulation[6], the Central Bank expects all regulated firms to have regard to the following definition,

[5] **N.B.** Regulated firms who are in scope for the EBA Guidelines on Outsourcing must comply with those guidelines at a minimum.

[6] Available legislation (at the time of publication of this guidance) includes, inter alia, the EBA Guidelines on Outsourcing Arrangements (EBA/GL/2019/02), the Directive 2014/65/EU (Markets in Financial Instruments Directive; MiFID II), the European Union (Insurance and Reinsurance) Regulations 2015 (Solvency II Regulations), the EIOPA Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002), the Credit Union Act 1997 and the Central Bank of Ireland Credit Union Handbook.

derived from the EBA Guidelines on Outsourcing, when determining the criteria for criticality or importance of the Function(s) to be outsourced:

"Functions that are necessary to perform core business lines or critical business functions should be considered as critical or important, unless the institution's 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 operational continuity of the core business line or critical business function".

The specific criteria to be considered by regulated firms, as applicable to them, under each of the relevant pieces of legislation, regulations or guidelines (as of the date of publication of this guidance), are, for ease of reference, contained at Appendix 2 to this guidance.

In respect of the assessment of criticality or importance of activities or functions, the Central Bank expects that regulated firms:

a) Have a defined methodology for determining the 'criticality or importance' of service which:

   i. clearly sets out the criteria/ factors that are considered in making this determination and the rationale for same;
   ii. can be applied consistently across all outsourcing decisions and is in line with relevant sectoral regulations and guidance; and
   iii. considers the nature, scale and complexity of the firm's business;

b) Document the methodology and any related definitions of critical or important in the regulated firm's outsourcing policy, which should be approved by the board;

c) Review the methodology/ definition periodically in conjunction with the outsourcing policy (See Part B Section 4.2);

d) As criticality or importance may vary throughout the lifecycle of an outsourcing arrangement, the assessment of criticality or importance should be reviewed periodically in order to ensure the categorisations remain appropriate. It is recommended that such reviews be conducted at a minimum:

   i. prior to signing an outsourcing contract or written outsource agreement;
   ii. at appropriate intervals thereafter e.g. during scheduled review periods;
   iii. where a regulated firm plans to scale up its use of the service or dependency on the OSP; and/or
   iv. if an organisational change at the OSP or a material sub-outsourced service provider takes place, including a change of ownership or to their financial position.

2. Intragroup Arrangements

Regulated firms are outsourcing activities and services from both intragroup entities and third party OSPs. The Central Bank acknowledges that outsourcing to intragroup entities can provide regulated firms with similar benefits to those provided by external third party OSPs but they can

also carry the same risks. Such benefits include, amongst others, the ability to consolidate expertise in 'Centres of Excellence' (COEs), as well as access to skills and resources at a group level, which may not otherwise be available to the local regulated firm. While the risks associated with intragroup and third party outsourcing are often similar in principle and comparable in nature, intragroup outsourcing can also present unique risks.

In respect of the assessment of intragroup outsourcing arrangements, the Central Bank expects that regulated firms:

a) Apply the same rigor when conducting intragroup outsource risk assessments as for third party OSP assessments;

b) Consider and be satisfied with the extent to which the regulated firm is in a position to exert sufficient influence on the group/or parent entity providing the service;

c) Consider and be satisfied with the application of the appropriate level of prioritisation of any remediation of outsourced services, where service outages may impact the regulated firm and/or the wider group;

d) Ensure that the resolution of any potential conflicts of interest is provided for in the governance arrangements; and

e) Assess if policies and procedures applied at group level are fit for purpose at the local Irish legal entity and that these policies and procedures comply with Irish legal and regulatory obligations on the Irish regulated firm.

3. Outsourcing & Delegation

The Central Bank notes that certain legislation, regulations and guidance[7] refer to use of 'delegation' in respect of the outsourcing of activities to OSPs. While the Central Bank considers that the obligations of such regulated firms with regard to outsourcing are well covered in the relevant sectoral legislation, regulations and guidance, the Guidance contained herein is relevant to such firms in assessing the adequacy and effectiveness of their outsourcing/delegation risk management frameworks. The aspects of the Guidance that address the management and security of a regulated firm's customer and business sensitive data (see Part B Section 5.2), in relation to the utilisation of CSPs, may be particularly relevant in this regard.

While the fulfilment of certain obligations may be conducted by the delegate on the firm's behalf, the regulated firm remains ultimately accountable. In respect of the assessment of delegation arrangements, the Central Bank expects that regulated firms:

a) Take note that "delegation" and "outsourcing" are not considered by the Central Bank to be different concepts;

[7] Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010; Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS); Central Bank of Ireland Fund Management Companies Guidance 2016.

b) Treat delegated arrangements to the same onerous due diligence, oversight and monitoring as for other outsourcing arrangements;

c) Have satisfied themselves that appropriate governance and risk management measures are in place in respect of their delegated arrangements and that these function effectively; and

d) Are able to demonstrate to the Central Bank that they have appropriate oversight of delegation arrangements and can evidence that the risks associated with outsourcing/delegation have been appropriately considered by the board and are being managed effectively.

4. Governance

4.1 The role of the board and senior management

Boards and senior management[8] of regulated firms are responsible for all activities undertaken by the regulated firm. As outlined above, this responsibility includes outsourced activities where the activities are conducted on the regulated firm's behalf by any third party, including any group entity. The board and senior management of regulated firms are ultimately accountable for the effective oversight and management of outsourcing risk within their business. This includes ensuring that the appropriate structures are in place to facilitate a comprehensive view and oversight of their outsourcing universe. Such oversight is a key element in assisting boards of regulated firms to address their responsibilities with regard to the security and resilience of service provision. While the performance of functions and activities can be outsourced, boards and senior management of regulated firms cannot outsource their responsibilities.

To ensure effective governance and oversight of outsourcing risk, the Central Bank expects that the board, senior management or management body (referred to below as "the board") of regulated firms:

a) Have taken appropriate action to ensure that the governance and risk management of their outsourcing frameworks is appropriate and operating effectively so as to fulfil their responsibilities for the management of outsourcing risk and is in line with the supervisory expectations set out in this Guidance[9];

b) Have a documented outsourcing strategy in place, which is aligned to the regulated firm's business strategy, business model, risk appetite, and risk management framework. The outsourcing strategy should be supported through appropriate policies, procedures and controls. Existing outsourcing risk management frameworks should be updated to ensure expectations set out in this Guidance[14] are appropriately considered and addressed;

c) Ensure that their outsourcing governance and risk management structures are in line with relevant sectoral legislation, regulation and guidelines particularly where functions are

[8] Please refer to Section 1.6 'Definitions'.
[9] In addition to any existing or future requirements under sectoral legislation, regulations or guidance.

outsourced to an OSP, whether third party or intragroup, operating in a different jurisdiction;

d) Ensure that outsourcing does not impede the regulated firm's ability to meet the conditions with which it must comply in order to remain authorised, including any conditions imposed by the Central Bank;

e) Maintain at all times sufficient substance and do not become 'empty shells' or letter-box entities';

f) Have a comprehensive outsourcing policy in place, in line with Part B Section 4.2, which is reviewed and approved by the board at least annually;

g) Assign responsibility for oversight of outsourcing risk and outsourcing arrangements to an appropriately designated individual, function and/or committee, to enable a holistic view of outsourcing to be maintained and reported on. This designated function should be directly accountable to the board;

h) Ensure that appropriate skills and knowledge are maintained within the regulated firm to effectively oversee outsourcing arrangements from inception to conclusion. This is especially important where the activities being outsourced are technical and/or complex in nature, for example in the case of outsourcing to CSPs;

i) Have appropriate and effective governance and internal controls to identify, measure, manage, monitor and report the risks associated with their outsourcing arrangements;

j) Ensure a methodology for determining the 'criticality or importance' of services (as detailed in section 2) is in place, which is assessed and approved by the board on a regular basis, to ensure it remains fit for purpose and is applied consistently across all outsourcing decisions;

k) Establish an outsourcing register in line with Part B Section 10.2, to identify and facilitate appropriate oversight and awareness of current and proposed outsourcing arrangements, and the associated risks, including the extent of the regulated firm's dependence on critical OSPs;

l) Ensure that there are appropriate structures and mechanisms in place to provide a comprehensive view of the regulated firm's outsourcing universe to the board, including the provision of timely and appropriate management information (MI) which provides sufficient detail to enable the board to challenge the establishment and ongoing oversight of outsourcing arrangements. Any review of outsourcing practices should include outsourcing arrangements already in place, as well as any proposed new arrangements; and

m) Ensure that outsourcing arrangements do not create impediments to the resolvability of the regulated firm.

4.2 Strategy and Policy for Outsourcing

As highlighted in Part A Section 2, the decision to outsource can result in many benefits for regulated firms including, reduced costs, increased efficiencies and access to skills, knowledge and technology that could be difficult, time consuming or costly to develop in-house. However,

decisions regarding outsourcing of particular activities or functions should not be taken in isolation or by disparate business functions within a regulated firm.

It is important that regulated firms consider their overall approach and strategy in relation to outsourcing and how it aligns with their overall business model, strategy and risk appetite. This is particularly important in order to inform board awareness and provide context for control of the regulated firm's outsourcing universe. The Central Bank expects that:

a) In line with Part B Section 4.1 above, regulated firms have a documented Outsourcing Strategy in place which is aligned to the regulated firm's business strategy, business model, risk appetite and risk management framework;

b) In formulating their outsourcing strategy, consideration is given to areas including but not limited to:

   i. the extent of outsourcing that they intend to undertake;

   ii. the types of activities and functions they will consider outsourcing;

   iii. the risks to the regulated firm, which arise from its outsourcing arrangements; and

   iv. the extent to which the firm has the skills and capacity to monitor and exercise oversight of outsourcing arrangements.

c) In the context of information and communications technology (ICT) that regulated firms' strategy considers what services and ICT operations they are retaining within the organisation and the different risks associated with outsourcing, particularly in the case of cloud based offerings. A regulated firm's choice should be aligned not only to its operational needs and operational risk appetite but also its capability to oversee and manage the cloud outsourcing arrangements once entered into;

d) Regulated firms can clearly evidence how any related risks will be managed and mitigated;

e) Regulated firms' outsourcing strategy informs a comprehensive outsourcing policy which is approved by the board.

It is crucial that regulated firms have a documented firm-wide Outsourcing Policy, which is reviewed and approved by the board at least annually. The Central Bank expects that the policy should address at a minimum:

a) The regulated firm's risk appetite as it relates to outsourcing;

b) Roles and responsibilities within the regulated firm for the oversight and management of outsourcing risk, including:

   i. the responsibilities of the board and the extent of its involvement in providing direction and decisions relating to outsourcing; and

   ii. the responsibilities of business lines and internal control functions with regard to outsourcing;

c) The criteria and methodology for the identification and classification of outsourcing arrangements as critical or important as discussed in Part B Section 1 above;

d) The approach to the identification, assessment, mitigation and management of risks associated with outsourcing as set out in Part B Section 5 below;

e) The approach to initial and ongoing due diligence on OSPs and the ongoing management, monitoring and review of outsourced arrangements in place;

f) The process for approval of new outsourcing arrangements;

g) The requirement to establish contracts, written agreements and SLAs as detailed in line with section 8;

h) The regulated firm's policy with regard to sub-outsourcing and whether this will be permitted under their contractual arrangements with their OSPs, particularly with regard to critical or important functions or material parts of such functions;

i) The approach to identifying and addressing potential conflicts of interest which may arise between the regulated firm and the OSP, particularly in the case of intra-group arrangements;

j) Details of the outsourcing risk management framework and structures for operational oversight and controls including:

   i. The frequency, approach and rationale underpinning regular review of the performance levels of OSPs;

   ii. The procedures for notification of changes to an outsourcing arrangement or the OSP, and for responding to such notifications;

   iii. The arrangements for independent review and audit to assess compliance with the relevant legal and regulatory requirements; and

   iv. The decision points and escalation routes for provision of management information (MI) to the board to enable the board to provide sufficient challenge prior to the approval of an arrangement and facilitate the ongoing oversight of arrangements.

k) The approach to business continuity arrangements as they pertain to the outsourcing arrangements;

l) The requirement for a documented exit strategy for each outsourcing arrangement deemed critical or important;

m) The termination processes, including consideration of unexpected termination of an outsourcing arrangement and the necessary contingency arrangements to effect a substitution of an OSP or implementation of the exit strategy;

n) The approach to safeguarding and maintaining the integrity of the regulated firm's data and systems as set out in their Data Management Strategy (see Part B Section 5.2 below);

o) The documentation and record keeping requirements in relation to outsourcing arrangements.

p) Any differences in the regulated firm's approach to the governance and management of:

   i. Critical or important outsourcing arrangements and other outsourcing arrangements;

   ii. Outsourcing to regulated OSPs versus non-regulated OSPs;

   iii. Outsourcing to an intra-group OSP versus external third party OSP;

   iv. Outsourcing to OSPs located within the EU/EEA and those located in third countries.

4.3 Record Keeping (Documentation Requirements - Register/s)

The Central Bank is of the view that the maintenance of appropriate records (database/register) in relation to a regulated firm's outsourcing universe, facilitating its centralised oversight and management of all outsourcing arrangements, is essential in managing the related risks appropriately.

The Central Bank has set out specific expectations in relation to the maintenance of outsourcing registers in Part B Section 10 below. Section 10 also outlines requirements for the submission of such registers to the Central Bank via an online regulatory return either cyclically or upon request, depending on the nature, scale and complexity of the firm's business and the extent of its reliance on outsourcing as part of its business model.

4.4 Outsourcing of Risk Management and Internal Control Functions

The Central Bank expects that the board and senior management of a regulated firm must, at all times, be fully responsible and accountable for the setting of a firm's strategies and policies (including the risk appetite and risk management framework). One of the key risks related to outsourcing of risk management and or internal control functions is loss of visibility and control.

In respect of the outsourcing of any part of their risk management or internal control functions, the Central Bank expects that regulated firms:

a) Be able to demonstrate to the Central Bank that the regulated firm has carefully considered the outsourcing risks of such functions and that the board or senior management of the regulated firm has satisfied itself that there are no significant concerns about the governance, risk management or internal control arrangements;

b) Maintain adequate oversight of these functions;

c) Apply due care and attention when considering and appointing the outsourcing of Pre-Approval Controlled Functions (PCFs) and Controlled Functions (CFs)[10];

d) Note that the regulated firm remains responsible for compliance with its obligations and that any outsourcing of PCF or CF roles does not therefore, diminish the responsibility of the board or senior management in this regard.

[10] Section 5 of The Central Bank's Guidance on Fitness and Probity Standards 2018 ("the F&P Guidance") and the Central Bank's Guidance on Fitness and Probity for Credit Unions provide guidance in relation to the outsourcing of PCFs and CFs.

5. Outsourcing Risk Assessment & Management

Effective monitoring, management and mitigation of outsourcing risk, requires the development, implementation and robust application of a strong outsourcing risk management framework. Comprehensive risk assessments are a key tool in enabling appropriate and adequate oversight of outsourced activities. This includes ensuring that risks inherent in all outsourced functions, activities, processes and systems are appropriately identified, measured, monitored and managed.

When developing their outsourcing risk management framework and conducting outsourcing risk assessments, the Central Bank expects that regulated firms:

a) Ensure that their risk management framework appropriately considers any outsourcing arrangements and that outsourcing risk is reflected in the regulated firm's overarching risk register;

b) Conduct comprehensive risk assessments in respect of any proposed outsourcing arrangement. Such risk assessments should be conducted prior to entering into such an arrangement;

c) Ensure that outsourcing risk assessments are tailored to take account of specific risks associated with outsourcing including but not limited to:

   i. Sub-outsourcing risks (in line with Part B Section 5.1 which follows);

   ii. Sensitive data risks (in line with Part B Section 5.2);

   iii. Concentration risks, including over-dependence on a single or small number of OSPs who cannot easily be substituted (in line with Section 5.3);

   iv. Offshoring risks (in line with Section 5.4);

   v. Step-in risk, which is the risk that the regulated firm may need to 'step-in' to provide financial support to an OSP in distress or to take over its business operations;

   vi. Business continuity risks and threats to the regulated firm's operational resilience through its dependence on OSPs. This is particularly relevant where there are limited or no alternate service providers to whom the outsourced activities can be transferred in a timely and orderly manner if the need arises (see Part B Section 9, which deals with BCP, Exit Strategies and Substitutability);

   vii. Legal, regulatory and reputational risks to which the regulated firm may be exposed in respect of the outsourced services; and

   viii. Any specific risks associated with cloud outsourcing, such as the movement of legacy systems to the cloud, the use of multi-tenanted environments, and cyber risk.

d) Consider and document the controls to be put in place to minimise exposure to any risks identified and that these controls and the mechanism for monitoring their effectiveness, are reflected in the relevant outsourcing contracts and SLAs;

e) Regularly review their outsourcing arrangements, with particular focus on their critical or important arrangements. Such reviews should consider whether:

   i. The nature, scale or complexity of the outsourced function or the risks associated with it have changed since its inception or last review;

   ii. Any such changes impact the firms assessment of the criticality or importance the function and whether the related risks and controls need to be updated accordingly; and

   iii. There have been any changes in the regulated firm's exposure to concentration risk either directly via their OSPs or through the introduction of or changes to sub-outsourcing arrangements.

f) Review and refresh their risk assessments on a periodic basis, to ensure that in the case of each firm, they continue to accurately reflect the regulated firm's business, including for example, its operating environment, legal or regulatory environment and to ensure they remain reflective of the current risks to which the regulated firm is exposed. Events which may trigger a review of outsourcing risk assessments may include:

   i. Scheduled reviews, in line with the regulated firm's outsourcing policy;

   ii. Changes to the nature or extent of the arrangement with OPSs, including where such changes result in an increased dependency on the OSP;

   iii. Changes to the circumstances of the OSP including organisational or financial changes; or

   iv. Identification by the regulated firm of deficiencies in the provision of the service by the OSP or notification of any significant breaches on the part of the OSP.

5.1 Sub-Outsourcing Risk

Sub-outsourcing can complicate the effective management of outsourcing risk. Parties to the chain in a sub-outsourcing arrangement can be spread across different physical and geographical locations, which can hinder a regulated firm's visibility and a regulator's supervisibility of activities being performed. 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. As highlighted below (see Part B Section 5.3 on concentration risk) concentrations may also develop in respect of sub-outsourced providers, which the regulated firm does not have sight of.

In order to effectively manage the risks associated with sub-outsourcing, the Central Bank expects that:

a) Regulated firms determine their appetite for sub-outsourcing as part of their outsourcing policy and actively manage the associated risks via their contractual arrangements and monitoring and oversight mechanisms;

b) Specific provisions relating to sub-outsourcing are included in contractual arrangements between regulated firms and OSPs in line with section 8 (Contractual Arrangements);

c) Sub-outsourcing risk arising from intragroup arrangements is treated in the same manner as that with external third party OSPs;

d) Regulated firms monitor sub-outsourcing of critical or important functions, or parts thereof, for any exposure to concentration risks related to the sub-outsourced service providers;

e) Regulated firms ensure at a minimum that the OSP oversees and manages the activities of the sub-outsourced service provider to ensure the fulfilment of all services in line with the original outsourcing contract and relevant SLAs;

f) In the case of sub-outsourcing of critical or important functions regulated firms should themselves apply an appropriate level of monitoring of the sub-outsourced service providers in line with their outsourcing risk assessment; and

g) Regulated firms should not agree to sub-outsourcing unless the sub-contractor agrees to:

   i. Comply with the relevant laws, regulatory requirements and contractual obligations; and

   ii. Provide the regulated firm and the Central Bank the same contractual rights of access and audit as those granted by the primary OSP – see Part B Section 7.3 for further detail.

5.2 Sensitive Data Risk

Outsourcing generally involves the handling of a regulated firm's data by a third party in order to execute the services contracted under the outsourcing arrangement. In many cases, this includes sensitive data, which is information that should be protected against unwarranted disclosure. In order to prevent data breaches or unauthorised disclosure of customer, employee or commercially sensitive data, firms need to implement effective measures for the appropriate storage, management, retention and destruction of this data.

In order to effectively manage risks relating to the potential loss, alteration, destruction or unauthorised disclosure of their sensitive data, the Central Bank expects regulated firms to:

a) Implement appropriate measures to secure and protect their data and to set out these measures in the firm's outsourcing policy and the contracts/written agreements governing outsourcing arrangements particularly for critical and important services;

b) Have, as good practice, 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 including when offshored, which may give rise to heightened data protection concerns. The Central Bank expects the data management strategy to:

   i. define an approach to data security and management, which ensures consistency of application by both the firm and the OSP/CSP (This is referred to as the "shared

responsibility model" in the context of cloud outsourcing – where day-to-day operational responsibility is shared between the CSP and the regulated firm)[11];

ii. address, in terms of location, data at rest, data in use and data in transit/transmission;

iii. consider and document data issues that might arise in the event of termination, insolvency and or recovery / resolution events;

iv. set out the standards and requirements to be applied in respect of the regulated firm's data including back-up and recovery, security protocols and encryption standards, access management and legal requirements;

v. ensure that, where data is encrypted, regulated firms make provisions to guarantee that any encryption keys or other forms of authentication are kept secure and accessible to the Central Bank; and

vi. in respect of cloud outsourcing, assess and document the risks in respect of any multi-tenanted environment[12] and the implications arising for monitoring and management of the arrangement.

c) Have regard to the requirements of available guidelines[13] or best practice frameworks in the context of information and data security from both a physical and logical perspective;

d) Ensure adherence with the requirements of any data protection legislation, including the GDPR, which apply to the operations of the firm. These considerations are particularly important when assessing the risks associated with offshoring especially outside the EU/EEA area;

e) Give due consideration, when conducting risk assessments, to the data characteristics of confidentiality, integrity, availability and authentication of data and information required to deliver outsourced business or service functions. These considerations apply to data and information both in hardcopy and digital formats. This is particularly important when the business or service functions are deemed critical or important; and

f) Design a comprehensive security architecture, the implementation of which may fall to both the regulated firm and related OSPs. Standards for configuring cloud services should ensure consistency of application of security measures both on own premises and in the cloud. In order to meet this control objective, regulated firms need to understand the different cloud deployment models, i.e. public/private/hybrid/community, and the service offerings available to them, which might include any or all of the following:

i. software as a service (SaaS);

ii. infrastructure as a service (IaaS); or

[11] However, overall responsibility for the oversight of IT operations and its security in respect of Confidentiality, Integrity, Availability and Authenticity (CIA^2) remains with the board of the regulated firm.
[12] This refers to software architecture on which a single instance of the software together with its supporting infrastructure runs on a server and serves multiple customers (tenants).
[13] Inter alia the EBA /GL/2019/04 - EBA Guidelines on ICT and Security Risk Management or the Central Bank's CBI Cross-Industry Guidance in respect of Information Technology and Cybersecurity Risks 09/2016.

iii. platform as a service (PaaS).

5.3 Data Security – Availability and Integrity

Regulated firms are critically dependent on the ready availability and integrity of their business and customer data. The requirement to ensure the availability and integrity of data drives the requirements for secure transmission, storage and backup arrangements. When considering backup arrangements regulated firms need to consider the measures necessary to ensure that data is ring-fenced offline and protected against corruption.

The Central Bank expects regulated firms to ensure implementation of appropriately designed and operationally effective controls for data-in-transit, data-in-memory and data-at-rest whether the controls are implemented by the regulated firm or an OSP on the regulated firm's behalf. These controls should include a mix of preventative and detective measures, including the following:

a) Configuration management;

b) Encryption and key management;

c) Identity and access management (which should include stricter controls for system administrators whose privileges and responsibilities can give rise to heightened risks in the event of unauthorised access), bearing in mind the requirements of a "shared responsibility model" if it applies in the case of cloud outsourcing;

d) Access and activity logging;

e) Incident detection and response;

f) Loss prevention and recovery;

g) Data segregation (if using a multi-tenant environment – Cloud or other);

h) Operating system, network and firewall configuration;

i) Staff training;

j) The ongoing monitoring of the effectiveness of the OSP's controls, including through the exercise of access and audit rights and the regular monitoring of reporting under the SLAs;

k) Policies and procedures to detect activities that may impact firms' information security (e.g. data breaches, incidents or misuse of access by either firm staff or third parties) and respond to these incidents appropriately (including appropriate mechanisms for investigation and evidence collection after an incident);

l) Procedures for the deletion of regulated firm data from all the locations where the OSP/CSP may have stored it following an exit or termination, provided that access to the data by the regulated firm or the Central Bank is no longer required; and

m) Contractual rights to audit the OSP data storage and management systems to ensure they are aligned with the regulated firm's data management requirements, policies and standards (in line with the contractual provisions set out at Part B Section 7.3).

5.4 Concentration Risk

In an outsourcing context, concentration risk is the probability of loss arising from a lack of diversification[14] of OSPs. Concentration risk can arise where a regulated firm develops a dependency on a single or small number of OSPs for the provision of critical or important activities or functions. It can also arise at a sectoral level where there are a limited number of providers for a sector or across sectors thus giving rise to problems of substitutability. In this context, concentration risk in cloud services is an emerging and increasingly significant issue. This is because large suppliers of IT and cloud services can become a single point of industry failure when many firms rely on the same provider[15]. It is also worth noting that in some cases, CSPs may hold significant leverage, due to the specialist nature of the services provided.

It is important to note that concentration risk can arise from outsourcing to intragroup entities, as well as to third party OSPs. Regardless of whether regulated firms are outsourcing to third party OSPs or intragroup, when assessing the risks of an outsourcing arrangement, regulated firms need to be aware of, manage and mitigate against any potential risks arising from outsourcing to a dominant, non-easily substitutable OSP or from outsourcing multiple services to one, or related OSPs[16].

Concentration risk not only arises directly from outsourcing arrangements but also indirectly from any sub-outsourcing undertaken by the OSP. While a regulated firm may consider it has adequately diversified the delivery of key processes to different OSPs, each of those OSPs may in turn be outsourcing the process, or a key element of the process to the same subcontractor. In this case, a regulated firm may be partially insulated from a failure by one of the OSPs but remains exposed to failure by the underlying sub-contractor.[17].

In order to monitor and manage this risk, the Central Bank expects regulated firms to:

a) Regularly assess and take appropriate measures to recognise and manage:
    i. Overall exposure and reliance on OSPs and sub-contractors; and
    ii. Concentration risks or vendor lock-in at firm or group level, due to multiple arrangements with the same or closely connected service providers or arrangements with OSPs where there is a substitutability issue ;

b) Ensure their risk management framework includes their approach to concentration risk identification, management, and reporting, which are appropriate in the context of the nature, size, and complexity of the regulated firm;

c) Ensure that their ability to negotiate and secure robust arrangements with such providers is not hindered, even in scenarios where there are a limited number of OSPs/CSPs to choose

[14] BITS Guide to Concentration Risk in Outsourcing Relationships
[15] EBA Guidelines on Outsourcing Arrangements EBA GL/2019/02
[16] EBA Guidelines on Outsourcing Arrangements EBA GL/2019/02
[17] BITS Guide to Concentration Risk in Outsourcing Relationships

from. Regulated firms should endeavour to secure satisfactory contractual terms from OSPs and reinforce them with appropriate SLAs and monitoring;

d) Include conditions in the outsourcing contract/written agreement that require the prior approval of the outsourcing institution to the possibility and modalities of sub-outsourcing – see Part B Section 7 Contractual Arrangements); and

e) Evaluate elements of concentration risk and evidence such in the risk assessments and due diligence review when outsourcing critical or important functions. These considerations should include:

   i. Single firm concentration of multiple services at same OSP or intragroup service provider;

   ii. Lack of substitutability issue arising from single service provider in the marketplace;

   iii. Multiple number of regulated firms outsourcing to same OSP either on a sectoral or cross sectoral basis;

   iv. Concentration risk arising from chain outsourcing (sub-outsourcing/sub-contracting) arrangements;

   v. Concentration risk arising from outsourcing to offshore jurisdictions; and

   vi. Contribution to systemic outsourcing concentration risk, which the Central Bank is obliged to monitor from a financial stability perspective.

5.5 Offshoring Risk

Outsourcing to offshore jurisdictions by regulated firms poses particular risks, some of which can significantly complicate both a regulated firm's and the competent authority's ability to ensure effective oversight and supervision [18]. Decisions with regard to offshoring, the risk appetite for same, and its oversight should be a matter for the board, the management body or senior management of the regulated firm and such decisions should be formally documented.

When considering or engaging in outsourcing to offshore jurisdictions, the Central Bank expects regulated firms to:

a) Evaluate the particular risks associated with countries to which they are planning to outsource activities ensuring that their outsourcing risk assessments pay sufficient attention to 'country risk' and document the assessment. In assessing country risk, the Central Bank expects that regulated firms give consideration to and take steps to mitigate the following concerns and or risks:

[18] When surveyed in late 2017 firms reported offshoring to some eighty plus countries across the globe. Significantly, 51% of these arrangements were reported to be with OSPs located outside the EEA.

i. Regulatory environment – the strength and expertise of financial services regulatory regime in operation in the OSPs' jurisdiction;

ii. Legal risk – in particular differences in insolvency regimes, trade, tax and employment laws;

iii. Political climate risk – risk of political agenda and/or instability and potential impacts on the ability of the OSP to continue providing service;

iv. Physical climate risk – risk of offshore location being subject to extreme weather or other environmental events such as pandemics and potential impacts on ability of the OSP to continue providing service;

v. Cultural or language issues – lack of understanding/misunderstanding of expectations and/or issues arising from the outsourced arrangement;

vi. Time-zones – ability to ensure availability of the relevant OSP personnel to deal with service issues in a timely manner; and

vii. Employment conditions in offshore jurisdictions – regulated firms should pay careful attention to taxation issues, labour laws and human rights and take into account the impact of their outsourcing on all stakeholders; this includes taking into account their social and environmental responsibilities.

b) Ensure that contracts for outsourced arrangements, including those which are offshored, stipulate that regulated firms and the Central Bank must be given access to carry out all necessary quality assurance and supervisory work (see also Part B Section 7 re Contracts and Written Agreements);

c) Ensure that there are minimum standards in place at the OSP in respect of risk appetite that are aligned to the regulated firm's risk management expectations and requirements to mitigate reputational risks or regulatory breaches;

d) Ensure that issues identified as part of the country risk assessment are also considered as part of the regulated firms disaster recovery (DR)/ BCP and substitutability planning; and

e) Pay particular attention to the jurisdictional and other complications, which might arise in the event of insolvency (e.g. recovery of data and records, protection of intellectual capital), termination and or recovery and resolution actions.

5.5.1 Potential Constraints on Offshoring

Regulated firms may, if appropriate, be restricted from offshoring activities, where for example, supervisibility is either severely constrained or non-existent. Such constraints could arise where there is no College of Regulators, no Memorandum of Understanding (MoU) and little or no contact with regulators in the chosen jurisdiction. Additional constraints may result from the nature or location of any offshored activity, where this creates a barrier or impedes the ability of the Central Bank to appropriately supervise the activity, or where the operational risks associated with the offshoring of particular activities are deemed by the Central Bank to be excessive.

With regard to potential constraints on offshoring, the Central Bank expects regulated firms to:

a) Inform the Central Bank of circumstances where such issues (as outlined above) may arise before committing to any offshoring arrangements in respect of the outsourcing of critical or important functions or services.; and

b) Assess the criticality or importance (see Part B Section 1 above) of proposed outsourcing arrangements at an early stage such that firms can inform (by way of notification to) and engage in dialogue with the Central Bank in sufficient time to permit appropriate supervisory consideration of the risks associated with the proposal.

6. Due Diligence

The Central Bank expects that appropriate and proportionate due diligence reviews will be conducted in respect of all prospective OSPs or intragroup providers, before entering into any arrangements.

With regard to critical and important functions, regulated firms should ensure that the OSP has the capabilities, and the appropriate authorisation, where required, to perform the critical or important function in a reliable and professional manner to meet its obligations over the duration of the contract.

In respect of due diligence, the Central Bank expects that regulated firms consider the following criteria when conducting the initial due diligence review in respect of OSPs:

a) The OSPs business model, nature, scale, complexity, financial situation, ownership and group structure;

b) The long-term relationships with OSPs that have already been assessed and perform services for the regulated firm;

c) Whether the OSP is a parent undertaking or subsidiary of the regulated firm, is part of the accounting scope of consolidation of the regulated firm, is a member, or is owned by firms that are members of the same group. In this context i.e. intragroup arrangements, consideration should be given to the extent of control or influence which may be exercised by the regulated firm;

d) Compliance with the General Data Protection Regulation (GDPR), Data Protection Act (DPA) and other applicable legal and regulatory requirements on data protection;

e) Whether the OSP is authorised by a regulatory authority to provide the service and whether or not the OSP is supervised by competent authorities;

f) Capacity of the OSP to keep pace with innovation within the market sector;

g) Business Reputation – including compliance, complaints and outstanding or potential litigation;

h) Financial performance;

i) Potential conflicts of interest, particularly in the case of intra-group arrangements ; and

j) The effectiveness of risk management and internal controls, including IT and cybersecurity in providing appropriate technical and organisational measures to protect the data in accordance with the firm's Data Management Strategy as referenced in detail at Part B Section 5.2 above.

In addition to the criteria listed above, the Central Bank expects that due diligence conducted by regulated firms also considers the:

a) Substitutability of the OSP/CSP (identifying possible alternative or back-up providers);

b) Potential exposure to concentration risk;

c) OSPs ability to demonstrate certified adherence to recognised, relevant industry standards;

d) Openness of the OSP to negotiating mutually acceptable contractual and SLA provisions;

e) Compatibility of the proposed arrangements with future development strategies of the regulated firm;

f) Managerial skills of the regulated firm to oversee the OSP and the skills within the OSP;

g) Employment and management of sub-contractors by the OSP;

h) Reliance by the prospective OSP on and control over sub-contractors;

i) Incident reporting and management programmes;

j) Insurance coverage;

k) Resilience measures;

l) Cross-border activities;

m) Track record of the OSP in respect of termination arrangements without having an impact on the continuity or quality of operations;

n) Ability of the OSP to meet its requirements and contractual obligations in relation to service quality and reliability, security and business continuity; in both normal and stressed circumstances;

o) Alignment of the risk appetite of the OSP with that of the regulated firm in order to avoid risk appetite breaches as a result of an OSP activity or failure. This may be avoided by both prior and ongoing assessment of the potential impact of outsourcing arrangements on operational risk appetite and risk tolerances as well as consideration of scenarios of possible risk events; and

p) Design and effectiveness of risk management controls at the OSP being at least as strong as the controls utilised by the regulated firm itself (i.e. they should meet the regulated firms control objectives).

These criteria outlined above should also be considered, as deemed necessary, in the course of periodic reviews of due diligence throughout the lifecycle of any contract.

6.1 Values and Ethical Behaviour – Regulatory Expectations

In line with EBA Guidelines on Outsourcing and general good practices, regulated firms are expected to

a) Take appropriate steps to ensure that OSPs act in a manner consistent with the values and code of conduct of the regulated firm; and

b) Satisfy themselves, in particular with regard to OSPs located in third countries and if applicable, their sub-contractors, that the OSP acts in an ethical and socially responsible manner and adheres to international standards on human rights (e.g. the European Convention on Human Rights), environmental protection and appropriate working conditions, including the prohibition of child labour.

6.2 Frequency of Due Diligence Review Performance

With regard to the frequency of due diligence reviews, the Central Bank expects regulated firms to:

a) Conduct an initial due diligence review as outlined in this section, that covers the breadth of operational and financial capacity of the OSP to provide and maintain a quality service to the outsourcing regulated firm;

b) Periodically[19] review the "financial health" of key OSPs, providing critical or important services, over the lifecycle of the contract. Even the largest of the OSPs can fail; and

c) Undertake / review a due diligence assessment prior to the expiry of key contracts in order to inform the decision of whether or not to renew the agreement. This should be performed sufficiently in advance of the termination / rollover date in order to permit the regulated firm sufficient time to either renegotiate the terms of the contract or undertake an orderly wind down or transfer of the arrangements.

7. Contractual Arrangements and Service Level Agreements (SLAs)

The Central Bank expects that arrangements with OSPs are governed by formal contracts or written agreements, preferably that are legally binding. These should be supported by Service Level Agreements (SLAs). Intragroup arrangements should be implemented at a minimum, by way of written agreements supported by SLAs. The adherence of OSPs whether external third parties or intragroup providers to contracts, written agreements and SLAs should be monitored by the regulated firm (see also Part B Section 8, which follows).

7.1 General Requirements

The Central Bank expects that, with regard to the contract or written agreement (and associated SLAs) governing the provision of critical or important functions or services, these should be

[19] For key OSPs of critical or important services a brief review of the financial health should be conducted each year.

resolution resilient and set out in line with EBA Guidelines on Outsourcing and general good practice to include the following provisions:

a) A clear description of the outsourced function or services to be provided;

b) The start date and end date (or renewal date, where applicable,) of the contract or agreement and the notice periods for the OSP and the regulated firm;

c) The governing law of the agreement i.e. the applicable jurisdiction for each agreement;

d) The parties' financial obligations;

e) Whether the sub-outsourcing of a critical or important function, or material parts thereof, is permitted and the conditions under which the sub-outsourcing is permitted. In this regard, the agreement should require OSPs to:

   i. notify regulated firms ahead of planned material changes to sub-outsourcing arrangements in a timely manner;

   ii. obtain prior specific or general written authorisation where appropriate;

   iii. give regulated firms the right to approve or object to material sub-outsourcing arrangements and/or terminate the agreement in certain circumstances; and

   iv. ensure that the regulated firm's and the Central Bank's rights of access and audit (see Section 8.3) apply in the case of any sub-outsourcing arrangement.

f) Specify any functions or activities that are prohibited from being sub-outsourced;

g) The location(s) (i.e. towns/cities, regions, and 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 regulated firm, in advance, if the OSP/CSP proposes to change the location(s);

h) Where control/custody of data is being outsourced, requirements regarding the accessibility, availability, integrity, confidentiality, privacy and safety of relevant data. (These should provide for appropriate and proportionate information security related objectives and measures including requirements such as minimum cybersecurity requirements, specifications of firms' data life cycle, and any requirements regarding data security management, network security and security monitoring processes, operational and security incident handling procedures including escalation and reporting);

i) Regulated firms 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;

j) The right of the regulated firm to monitor the OSP's performance on an ongoing basis by reference to Key Performance Indicators (KPIs) which should be set out in the associated SLAs;

k) The agreed service levels, which should include precise quantitative (measureable) and qualitative performance targets (using KPIs to track) 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;

l) The reporting obligations of the OSP to the regulated firm should require timely reporting against the KPIs, which provides actionable MI to the regulated firm. This should include communication by the OSP of any development that may have a material impact on the OSP'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, meeting the obligations to submit reports of the internal audit function of the OSP;

m) Whether the OSP should take out mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;

n) The requirements (on all parties) to implement and test business contingency plans (taking account of the regulated firms impact tolerances for the disruption of critical or important services);

o) Termination rights and exit strategies covering both stressed and non-stressed scenarios. As in the case of business contingency plans, both parties should commit to take reasonable steps to support the testing of regulated firms' exit strategies and termination plans – See also further detail relating to Termination Rights below;

p) Provisions that ensure that the data owned by the regulated firm can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the OSP/CSP;

q) The obligation of the OSP/CSP to cooperate with the Central Bank as prudential regulator and the resolution authority of the regulated firm including other persons appointed by them;

    a) to ensure resolution resiliency, for regulated firms, falling within scope of S.I. No. 289/2015 (the 2015 Regulations), which transposed Directive 2014/59/EU (BRRD) into Irish law, a clear reference to all relevant resolution authorities and the powers thereof especially to Articles 68 and 71 of Directive 2014/59/EU (BRRD)[20] as transposed by the relevant national competent authority, and in particular a description of the 'substantive obligations' of the contract in the sense of Article 68 of that Directive; and for firms

[20] Article 68 BRRD:
Without prejudice to the full provisions of Art. 68 of the BRRD, this article ensures that a crisis prevention measure or crisis management measure20 (defined in Art. 2 (101&102 BRRD), taken in accordance with the BRRD (or any transposing regulations), shall not be taken to mean that the institution (or any subsidiaries thereof) have undergone a default, insolvency, or any other similar event. Therefore, the taking of a crisis prevention or crisis management measure under the provisions of the BRRD, shall not lead to the triggering of insolvency or default type triggers within a contract, as long as the substantive obligations of the contract continue to be performed.
Article 71 BRRD:
Without prejudice to the full provisions of Art. 71 BRRD, this article refers to resolution authorities' powers to suspend the termination rights of any party to a contract with an institution that is under resolution.

which are not subject to any current or likely future resolution framework, this Guidance should be considered good practice;[21]

r) The unrestricted right of regulated firms and the Central Bank to inspect and audit the OSP/CSP with regard to, in particular, the critical or important outsourced function. See also Part B Section 7.3 Access, Information and Audit Rights below;

s) Contractual arrangements, in respect of outsourcing, should ensure that where a situation of Recovery and or Resolution arises it cannot be deemed to be grounds for termination of the outsourcing arrangements in respect of critical or important services by the OSP;

t) Document the nature of the "shared responsibility" model (within the SLA) if such arises in the implementation of the cloud service arrangements. This should also document the agreed data management strategy and any restrictions on the offshoring of data; and

u) As a matter of good practice, regulated firms should also consider the inclusion of the following in contracts or written agreements:

   i. Dispute resolution arrangements containing provisions for remedies including penalty clauses to be invoked if required in the event of significant breaches of KPIs in respect of critical or important services;

   ii. Indemnification;

   iii. Limits and liability;

   iv. Provisions for amendment of contracts or written agreements; and

   v. Notifications of financial difficulty, catastrophic events, and significant incidents.

7.2 Termination Rights

a) The contract or written agreement should expressly allow the possibility for the regulated firm to terminate the arrangement, in accordance with applicable law, including, inter alia, in the following situations:

   i. where the OSP is in breach of applicable law, regulations or contractual provisions;

   ii. where impediments capable of altering the performance of the outsourced function are identified;

[21] Further "good practice" as it relates to resolution and failure events:

In general, contracts should provide for events of resolution and/or failure of a regulated firm to be managed in an orderly manner by the relevant authority. Parties to contracts subject to a failure or resolution event should cooperate fully with the Central Bank of Ireland and generally should not trigger any termination clauses as long as the substantive obligations of the contract can continue to be met
Additionally, contractual arrangements should further provide for the ability for the resolution authority, the Central Bank of Ireland, and/or the firm itself to assign the agreement to another entity, following a sale, merger, or similar reorganisation to this entity, of all or a substantial proportion of the institution's assets or business activities, without the consent of the other party within a resolution scenario. This is again provided that, the substantive obligations of the contract can continue to be met.

iii. where there are material changes affecting the outsourcing arrangement or the OSP (e.g. sub-outsourcing or changes of sub-contractors);

iv. where there are weaknesses regarding the management and security of confidential, personal or other sensitive data or information e.g. a breach of agreed standards; and

v. where instructions to terminate are given by the Central Bank, e.g. in the case that the Bank is, as a consequence of the outsourcing arrangement, no longer in a position to effectively supervise the regulated firm.

b) The contract or written agreement governing the outsourcing arrangement should facilitate the transfer of the outsourced function to another OSP or its re-incorporation into the regulated firm. Consequently, the contract or written agreement should:

i. clearly set out the obligations of the existing OSP, in the case of a transfer of the outsourced function to another OSP or back to the regulated firm, including the treatment of data;

ii. set an appropriate transition period, during which the OSP, after the termination of the outsourcing arrangement, would continue to provide the outsourced function to reduce the risk of disruptions; and

iii. include an obligation on the OSP to support the regulated firm in the orderly transfer of the function in the event of the termination of the outsourcing agreement.

7.3 Access, Information and Audit Rights

a) Regulated firms should ensure within the contract or written outsourcing arrangement that the internal audit function is able to review the outsourced function using a risk-based approach.

b) The contract or written outsourcing arrangements, regardless of the criticality or importance of the outsourced function, should refer to the information gathering and investigatory powers of competent authorities and resolution authorities, as applicable, with regard to OSPs located in a Member State and should also ensure those rights with regard to OSPs located in third countries.

c) Regulated firms should ensure that within the contract or written outsourcing agreement, with regard to the outsourcing of critical or important functions the OSP grants them and their competent authorities, including resolution authorities, and any other person appointed by them or the competent authorities, the following:

i. 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 OSP's external auditors ('access and information rights'); and

ii. 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.

d) Regulated firms are expected to exercise their access and audit rights, determine the audit frequency and areas to be audited using a risk-based approach and in doing so adhere to relevant, commonly accepted, national and international audit standards.

7.4 Review of Agreements

a) Written agreements and contracts should be reviewed periodically, for example, when changes to the business model, the completion of risk assessments or regulatory change, warrants a reconsideration of the continued suitability of the contract.

b) Reviews should also be scheduled in sufficient time in advance of renewals or termination dates to ensure smooth transitions or continuity of service.

7.5 Non-Critical or Important Outsourcing Arrangements

a) Written agreements for non-critical or less important outsourcing arrangements should include appropriate contractual safeguards to manage relevant risks.

b) Regardless of criticality or importance, regulated firms should ensure that outsourcing agreements/contracts do not impede or limit the Central Bank's (or third parties appointed by it to exercise these rights) ability to effectively supervise or audit the regulated firm or its outsourced activity, function or service.

8. Ongoing Monitoring and Challenge

In conducting appropriate monitoring and challenge of the outsourcing framework, the underlying outsourcing arrangements and the operational functioning of same, regulated firms should incorporate outsourcing assurance into its three lines of defence.

8.1 Monitoring of outsourcing arrangements

Regulated firms are expected to put in place appropriate mechanisms to oversee, monitor, and assess the appropriateness and performance of their outsourced arrangements. Such mechanisms will generally be executed by the first line[22] of defence with oversight and challenge through the second line[23] in terms of performance against standards and effective management of the risk. In this regard, the Central Bank expects that regulated firms:

[22] First line – e.g. the business and operational functions that have responsibility for day to day engagement with and oversight of the performance of the OSP – the risk owners.
[23] The risk management and compliance functions within a regulated firm who provide assurance to the board and senior management that the risk is being managed effectively within the business.

a) Have sufficient and appropriately skilled staff within the organisation to oversee, interrogate, analyse and challenge the effectiveness of the outsourced arrangement (in line with Part B Section 4.1 (g) above);

b) Identify key decision makers who have the ability and capability to make decisions based on the information being provided;

c) Monitor the performance of the OSP using a risk based approach, including by:

   i. Ensuring receipt of appropriate reports from the OSP;

   ii. Assessing the performance of the OSP, including through the use of measures agreed and documented in their SLAs e.g. key performance indicators (KPIs), key control indicators (KCIs), service reviews and reports, outcomes of internal audit or other third party independent reviews commissioned by the OSP;

   iii. Assessing the adequacy of the OSPs business continuity measures and associated testing and the effectiveness of the integration with those of the firm, as detailed in Section 10 below; and

   iv. Conducting onsite reviews of the OSP.

d) Take appropriate measures to ensure that any deficiencies identified in the provision of the service by the OSP are effectively addressed, and if necessary escalated to ensure remediation. This may include an ultimate decision to terminate the arrangement; and

e) Incorporate assurance testing related to the management and monitoring of outsourcing as part of their risk management and compliance monitoring programmes. Such monitoring reviews as referred to above and assurance testing should be conducted on a frequency and to a degree commensurate with the nature, extent and criticality of the outsourcing arrangements engaged in by the regulated firms and its outsourcing risk assessment in respect of each of these arrangements. Firms should document the rationale, in its Outsourcing Policy, for the selected frequency of the conduct of such reviews and be in a position to provide this information to supervisors on request.

8.2 Internal Audit & Independent Third Party Review

Part B Section 8.1 above, refers to the day-to-day operational oversight of the performance of the OSP by the first and second line of defence. Regulated firms must also ensure that assessment of the effective performance of the arrangement and of the controls to mitigate associated risks, forms part of its third line of defence assurance programme, via its internal audit plan. In line with their outsourcing policy and risk assessment, regulated firms should also consider the circumstances in which independent external third party review may be necessary, in order to obtain satisfactory assurance regarding their outsourcing universe. The Central Bank expects that:

a) Using a risk based approach, the audit programme of the internal audit function assesses:

   i. That the regulated firm's outsourcing framework is operating effectively and in line with the outsourcing policy and the firm's risk appetite;

ii. Whether the outsourcing policy and associated control framework have been reviewed and updated to take account of any changes to the business, any new or emerging risks and any changes to the legislative or regulatory framework that impact on the firm's outsourcing universe;

iii. That outsourcing arrangements are being correctly classified in line with the regulated firm's methodology for the assessment of "criticality and importance". In this context, periodic assessment of the firm's methodology should also be conducted to ensure that it remains appropriate and fit for purpose, based on the firms business model, strategy and risk assessment;

iv. That the regulated firm's outsourcing register is being appropriately maintained to ensure accuracy and currency;

v. The adequacy and appropriateness of the firm's outsourcing risk assessment generally and it's application in respect of specific outsourcing arrangements;

vi. The effectiveness of the oversight and direction of the board, senior management or management body and any relevant committees in respect of outsourcing;

vii. The effectiveness of the regulated firm's monitoring and management of its outsourcing arrangements; and

viii. The operation by the OSP of the underlying outsourced activities or functions via onsite audits.

b) Regulated firms ensure that the party conducting the audit/review, whether internal or external, has the necessary skills and expertise to conduct the review effectively and to comprehensively assess and report on the outcomes. This is of particular relevance where the outsourcing arrangement presents a significant degree of technical complexity, for example in the case of outsourcing to cloud service providers (CSPs).

c) Regulated firms ensure that they have the appropriate skills and expertise to review, challenge and make informed decisions as to the quality and outcomes of any audit/review.

8.3 Use of Third Party Certifications and Pooled Audits

As part of their ongoing monitoring regime, regulated firms may utilise a number of different sources of information to aid their awareness and understanding of risks associated with their outsourcing arrangements and how these risks are managed. This may include independent third party reports and certifications provided by the OSP and onsite audits of the activities of the OSP. Onsite audits may be conducted by the internal audit function or a third party commissioned directly by the regulated firms (as referenced in Part B Section 8.2 above), or in appropriate circumstances onsite audits may also be conducted with other regulated firms (pooled audits). Where regulated firms utilise third party certifications provided by the OSP and/or pooled audits, the Central Bank expects that:

a) Regulated firms assess and document the circumstances in which third party certifications and pooled audits are deemed to provide appropriate levels of assurance, in line with their outsourcing policy and risk assessment. In this context, regulated firms must be mindful that the level of assurance required may be more onerous given the nature, scale and complexity of their business and the criticality and importance of the outsourced functions that are the subject of the review.

b) When utilising third party reports or certifications or availing of pooled audits, the regulated firm is satisfied and can evidence that:

   i. The scope and process for the review is appropriate, and provides sufficient coverage of the outsourced activities and functions and related risk management controls;

   ii. The review criteria are up to date and take account of all relevant legal and regulatory requirements;

   iii. The third party commissioned to conduct the review has the appropriate skills and expertise (in line with the general requirements relating use of independent third parties referenced in Part B Section 8.2 above); and

   iv. The regulated firm has the appropriate skills and expertise to review, challenge and make informed decisions as to the quality and outcomes of the review (in line with the general requirements relating use of independent third parties referenced in Part B Section 8.2 above).

c) Regulated firms ensure that their audit methodology enables them to fulfil their legal and regulatory obligations at all times, in particular as they relate to outsourcing risk management and operational resilience.

9. Disaster Recovery and Business Continuity Management

Key to effective governance and risk management associated with any outsourcing arrangement is ensuring continuity of services through robust disaster recovery (DR) and business continuity management (BCM). An integral part of the DR/BCM process is the regulated firm's resilience to an event occurring. Critical to this is the continuous assessment of the regulated firm's business processes and the DR and business continuity plans (BCPs) in place, to ensure that controls or other resilience measures are effective and in line with evolving practice and emerging risks and/or issues.

In order to ensure the robustness of a regulated firm's own DR and business continuity plans (BCPs), it is important that regulated firms consider the implications of having outsourced to an OSP and the BCM arrangements that the OSP has in place. It is important that there is close alignment of the DR/BCM arrangements of regulated firms and those of their outsource service providers (OSP), particularly where the OSP is involved in the delivery of critical or important functions and their related systems and data.

When designing and implementing disaster recovery and business continuity measures as they pertain to or include outsourced arrangements, the Central Bank expects that regulated firms:

a) Consider DR/BCM when proposing to engage the services of an OSP and ensure that service disruptions can be maintained within the impact tolerances and recovery time objectives (RTOs) of the firm as documented within its most recent Business Impact Analysis;

b) Ensure that when entering into an outsourcing arrangement, all governance surrounding such an arrangement, including business continuity plans and exit strategies (see section 10.1) are updated to reflect any implications of the outsourcing arrangement;

c) Document and implement business continuity plans in relation to their critical and important outsourced functions and that these plans are tested and updated on a regular basis.

d) Consider the need for the creation of periodic isolated "safe harbour" backup arrangements[24] in respect of cloud outsourcing arrangements as part of their business continuity planning, to ensure the preservation of data integrity and recovery in the aftermath of a major cyber event;

e) Ensure the OSP has a business continuity plan in place, which includes the resources (processes, systems, personnel etc.) required to fulfil the regulated firm's critical or important outsourcing arrangements;

f) Ensure that any critical or important outsourcing arrangement includes a requirement for the OSP to carry out testing of its own business continuity plans at least annually;

g) Ensure that they can participate in the OSPs business continuity plan testing, where necessary;

h) Conduct coordinated testing of these arrangements on a regular basis and report the results to the boards of both the regulated firm and the OSP;

i) Have sight of reports on business continuity measures and testing undertaken by the OSP and are informed of any relevant actions or remediation arising as a result of this testing, as appropriate;

j) Ensure that boards and senior management of the firm take remedial action to address any deficiencies identified in the performance of the OSP, either as part of coordinated testing of the regulated firm's business continuity measures, or via results of the OSP's own BCP testing. Such actions may include ultimate termination of the outsourced arrangement if such deficiencies persist;

k) 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;

l) Ensure that outsourcing arrangements are considered in the context of firms' recovery planning and resolution planning and that the operational continuity of critical functions is ensured including scenarios of financial distress or during financial restructuring or resolution.

[24] "Safe Harbour" in this case the term is used in respect of the creation of periodic isolated offline backup arrangements to ensure that there will always be a clean copy of critical data, available for recovery, whose integrity can be vouched for at a point in time.

When considering appropriate DR/BCP measures these considerations should be linked with the planning of Exit Strategies – See Section 9.1, which follows.

9.1 Exit Strategies

The resilience of any regulated firm to vulnerabilities presented by outsourcing arrangements will be largely dictated by the effectiveness of the contingency measures in place, including their exit strategies. As outsource service users, regulated firms should understand exit costs, the arrangements to be initiated and the legal and operational risk implications in the event of the termination of outsourcing contracts.

When entering into an outsourcing arrangement, the Central Bank expects regulated firms to consider and plan how the regulated firm would exit the arrangement for example in the case of:

a) Failure on the part of the OSP to provide the service to the requisite standard;

b) Unexpected termination of the arrangement dictated by the OSP/CSP;

c) Stressed circumstances on the part of the OSP such as hostile takeover, insolvency or liquidation; or

d) Any other circumstance that the regulated firm envisages may prompt it to exit the arrangement.

With regard to the development and maintenance of exit strategies associated with outsourcing arrangements, the Central Bank expects that regulated firms:

a) Have considered and documented their impact tolerances for business service interruptions and have in place a documented framework to identify and escalate breaches of these tolerances and procedures for dealing with same. This framework, (which may be linked to monitoring of performance against SLAs as detailed in Part B Sections 7 and 8 respectively), should include criteria and procedures for invoking an exit strategy where deemed necessary;

b) Have a clearly defined and documented exit strategy in place (in particular for their critical or important outsourcing arrangements), which is viable, appropriately planned, documented and regularly tested and takes into account at least the circumstances detailed in Part B Section 9.1 above;

c) Assess whether an OSP can be substituted. Where substitutability is established, regulated firms should seek to identify alternate OSPs and make appropriate assessments of the measures required to transfer to such alternate providers where an exit strategy must be invoked. Theses assessments should inform the regulated firm's exit strategy;

d) Ensure that the exit strategy includes arrangements for reintegration of services within the regulated firm or group entity, either where an alternative provider is not available or in cases where reintegration is required by regulation;

e) Consider, plan and test (insofar as is possible[25]) scenarios which may warrant the transfer of activities to another OSP or back in-house;

f) Develop and maintain skills and expertise so that functions can, if required, be taken back in-house by the regulated firm or transferred to an alternative provider in an orderly manner;

g) Ensure that the exit strategy estimates the timeframe for transfer of service either to an alternative provider, or if necessary, to take the service back in–house;

h) Consider and implement within their exit strategy, contingency arrangements to cover the interim period between invoking an exit strategy and the ultimate transfer. This is particularly important where the timeframe for transfer of service is significant;

i) Ensure appropriate understanding and oversight of the data flows between the regulated firm and the OSP, including how to manage any potential interruption of service or downtime to ensure that critical business functions remain available;

j) Have considered the potential for and implications of "step-in risk" materialising in the context of stressed scenarios. Regulated firms should determine the viability of invoking 'step-in' rights in such scenarios. The form that such 'step-in' would take should be determined, which may include providing financial support for, or takeover of the OSP. Where 'step-in' is deemed viable, it should be planned and documented as part of the exit strategy;

k) Periodically review and update exit strategies to take account of developments that may alter the feasibility of an exit in stressed or non-stressed circumstances. For example, new service providers or new technology tools which, particularly in the case of cloud outsourcing arrangements, may facilitate switching of service providers or locations and the portability of critical data and applications. These tools are constantly evolving, in particular in technology outsourcing, including Cloud, and may include:

   i. evaluation of new potential OSPs;

   ii. technology solutions and tools to facilitate the switching and portability of data and applications; and

   iii. adoption and adherence to industry codes and standards by the provider;

l) In the specific case of critical or important cloud outsourcing arrangements, assess the resilience requirements of the outsourced service and data and determine which of the available Cloud resiliency service options is most appropriate. These may include multiple availability zones, regions or service providers;

m) Ensure that in the case of intra-group arrangements, where regulated firm's avail of exit plans that have been established at a group level, that the plans address the expectations set out in this Guidance and relevant sectoral legislation and regulatory requirements.

[25] Testing should include at a minimum a detailed walkthrough of the process that would be invoked, which should be challenged by the board and senior management to ensure that it is feasible, and formally approved.

Regulated firms must ensure that such plans are viable and can be executed accordingly in respect of the regulated firm's critical or important outsourced arrangements.

10. Provision of Outsourcing Information to the Central Bank of Ireland

The Central Bank expects to be informed, by way of Notifications, by all firms in respect of proposed "critical or important" outsourcing arrangements as required by EBA/GL/2019/02 Outsourcing Guidelines, EIOPA BoS-14/253 Guidelines on System of Governance, EIOPA BoS-20-002 Guidelines Outsourcing to Cloud Service Providers, ESMA 50-157-2403 Guidelines on Outsourcing to Cloud Service Providers, sectoral regulation and/or as a matter of good practice.

This section sets out the Central Bank's expectations in respect of provision of information by regulated firms to the Central Bank in relation to their proposed and existing outsourcing arrangements. It sets out the Bank's expectations in respect of:

- Notifications and Reporting in respect of outsourcing related matters; and
- The Maintenance and Submission of Registers of Outsourcing Arrangements by way of regulatory return or as otherwise requested.

This section is supported by Appendix 3, which sets out the guidance in respect of the content (data elements) and completion of the Register/s.

These requirements relate to all firms regulated by the Central Bank of Ireland – Reference also Part A Section 4, which sets out the general applicability of this Industry Guidance and the factors relating to proportionality in its application.

10.1 Notifications[26] & Reporting[27]

10.1.1 Timing and Content of Notifications

In line with the EBA Guidelines on Outsourcing and other existing regulatory requirements and as a matter of good practice, the Central Bank requires timely notification of planned critical or important outsourcing arrangements[28] and of material changes to existing critical or important outsourcing arrangements.

[26] The Bank expects to be informed, in a timely manner of proposed critical or important outsourcing arrangements by way of Notification.

[27] This guidance also addresses aspects of proposed reporting requirements accepting that some may overlap with existing Operational Risk and or PSD/2 requirements.

[28] The written notification requirements set out in Article 49(3) of the Solvency II Directive and further detailed by EIOPA Guidelines on System of Governance are applicable, as are Regulation 51(3) of the European Union (Insurance and Reinsurance) Regulations, 2015, CBI Industry Paper 2016 – Notification Process, Regulation 18 of Central Bank (Investment Firms) Regulations 2017 and Fund Administrator Outsourcing Guidance, and the Credit Union Act 1997 and Credit Union Handbook. These requirements may change over time and it is the responsibility of individual firms to be vigilant to any changes and comply with the requirements.

Events, which could give rise to the necessity for Notification of proposed or changing outsourcing arrangements[29] include:

a) Licence Authorisation Requests, which include outsourcing arrangements of a critical or important nature;
b) Proposals for new critical or important outsourcing arrangements including sub-outsourcing;
c) Existing arrangements which have been redefined as critical or important;
d) Changes in outsourcing services providers and or locations for provision of critical or important services including the addition of sub-outsourcing providers;
e) Changes to the firm's business model – which include proposed new critical or important outsourcing arrangements;
f) Termination of critical and/or important outsourcing arrangements; and
g) In the event of Recovery and Resolution Processes, continuation/extension of existing outsourcing arrangements (maybe on a temporary basis) or the firm's intention to terminate and the manner of termination of arrangements.

The Central Bank expects regulated firms to assess the criticality or importance of proposed outsourcing arrangements at an early stage such that they can inform (by way of notification to) and engage in dialogue with the Central Bank in sufficient time to permit appropriate supervisory consideration of the risks associated with the proposal. In this context, firms may be requested to:

- Provide additional information to supervisors if sought such as the output from due diligence and or risk assessments conducted or other as specified;
- Enhance its due diligence review, upgrade its governance and or risk management arrangements and delay entering into an agreement until such are satisfactory;
- Amend proposed contracts, written agreements or SLAs to ensure regulatory compliance and ensure delivery on risk management expectations.

In particular, the Central Bank expects firms to bring to the Central Bank's attention proposals to outsource any of its critical or important functions or services to offshore jurisdictions in sufficient time, and prior to the commencement of any outsourcing arrangement of critical or important functions or activities, to consider the risks, especially those relating to supervisibility.

The onus is on regulated firms to inform the Central Bank of circumstances where such issues may arise before committing to any offshoring arrangements in respect of the outsourcing of critical or important functions or services.

The Central Bank expects Notifications of proposed critical or important outsourcing arrangements to include, at least, the information specified in paragraph 54 of the EBA Guidelines on Outsourcing.

[29] It should not be inferred from the expectations relating to Notifications that the Central Bank is creating a pre-approval process, where such a pre-approval is not an existing legal requirement. The Guidance does not supersede existing sectoral legislation, regulations and guidance on outsourcing, but rather supports and complements them by setting out aspects of good practice for the effective management of outsourcing risk in all its forms.

The Notification should also include any additional information as may be required by sectoral guidelines applicable in respect of the regulated firm.

Paragraph 54 specifies content (data elements), which the firm will be expected to enter into its Register (Database) and it is that data that should form the basis of the Notification. It would be useful to also include, as available, some of the data, which is specified in paragraph 55, which also relates to the contents of the Register in respect of critical or important outsourcing arrangements.

The Notification of a proposed new critical or important outsourcing arrangement should contain the following data items, as available to the regulated firm, at the time of notification:

a) A reference number for the proposed critical or important outsourcing arrangement;

b) The proposed start date and, as applicable, the next contract renewal date, the end date and/or notice periods for the OSP and for the regulated firm if known;

c) A brief description of the outsourced function, including the data that will be outsourced and whether or not personal data will be transferred or if the processing of such data will be outsourced to a service provider;

d) A category assigned by the institution or payment institution that reflects the nature of the function as described under point (c) (e.g. information technology (IT), control function), which should facilitate the identification of different types of arrangements;

e) The name of the OSP, the corporate registration number, the legal entity identifier (where available), the registered address and other relevant contact details, and the name of its parent company (if any);

f) The country or countries where the service is to be performed, including the location (i.e. country and town or region) of the storage and or processing of data;

g) Brief summary of why the outsourced function is considered critical or important;

h) The date of the assessment of the criticality or importance of the outsourced function.

i) In the case of outsourcing to a cloud service provider (CSP), the cloud service and deployment models, i.e. public/private/hybrid/community, and the specific nature of the data to be held and the locations (i.e. countries and towns or regions) where such data will be stored and or processed;

j) The regulated firms within the scope of the prudential consolidation, that will make use of the outsourcing arrangement;

k) Whether or not the OSP or sub-service provider is part of the group or is owned by the regulated firm or other members within the group i.e. an intragroup arrangement;

l) The date of the most recent risk assessment conducted in respect of the proposed arrangement and a brief summary of the main results;

m) The individual or decision-making body (e.g. the management body) in the regulated firm that approved the proposed outsourcing arrangement;

n) The governing law of the proposed outsourcing agreement;

o) Where applicable, the names of any sub-contractors to which material parts of a critical or important function are sub-outsourced, including the country where the sub-contractors are registered, where the service will be performed and, if applicable, the location (i.e. country or region) where the data will be stored and or processed;

p) The outcome of the assessment of the service provider's substitutability (as easy, difficult or impossible), the possibility of reintegrating a critical or important function into the regulated firm or the impact of discontinuing the critical or important function;

q) Identified alternative service providers in line with point above;

r) Whether the proposed outsourced critical or important function supports business operations that are time-critical; and

s) The estimated annual budget cost of the outsourcing arrangement.

Regulated firms may be requested to supplement this information as outlined above.

10.1.2 Supervisory Response to Notifications

The Central Bank reserves the right, with respect to all sectors, to take appropriate action in respect of proposed critical or important outsourcing arrangements, in circumstances where it is identified that there is, for example, unacceptable risk posed to financial stability, the firm or its customers (either in course of the operation or termination of the service), or when there are major difficulties arising in respect of the supervisibility of the arrangements.[30] The Central Bank reserves the right to raise any regulatory or supervisory concerns, which arise in respect of outsourcing arrangements proposed by firms at any stage of the outsourcing lifecycle.

10.1.3 Reporting of Adverse Incidents etc.

Regulated firms should also report to the Central Bank when the following occur in respect of outsourcing arrangements:

a) Matters/events giving rise to a significant change to the outsourcing aspects of the business model;
b) When a material event occurs, which affects the provision of critical or important services by an OSP;
c) When material breaches of contractual arrangements or SLAs arise which affects the regulated firm in the conduct of its regulated services or adversely affects customers/consumers.

10.2 Maintenance and Submission of Registers

The Central Bank expects that each regulated firm will establish and maintain an outsourcing register.

[30] This may arise where The Central Bank deems that the proposed outsourcing arrangements could give rise to an unacceptable increase in exposure to operational risk for the firm.

The register should include at least the following information, (which is broadly in line with EBA, EIOPA and draft ESMA Guidelines), for all existing and future outsourcing arrangements so that it is maintained up-to-date:

a) A reference number for each outsourcing arrangement;

b) The start date and, as applicable, the next contract renewal date, the end date and/or notice periods for the service provider and for the institution or payment institution;

c) A brief description of the outsourced function, including the data that are outsourced and whether or not personal data (e.g. by providing a yes or no in a separate data field) have been transferred or if their processing (of personal data) is outsourced to a service provider;

d) A category assigned by the institution or payment institution that reflects the nature of the function as described under point (c) (e.g. information technology (IT), control function), which should facilitate the identification of different types of arrangements;

e) The name of the service provider, the corporate registration number, the legal entity identifier (where available), the registered address and other relevant contact details, and the name of its parent company (if any) the details should specify whether the OSP is a regulated firm and if so provide the name of the regulator;

f) The country or countries where the service is to be performed, including the location (i.e. country or region) of the data;

g) Whether or not (yes/no) the outsourced function is considered critical or important, including, where applicable, a brief summary of the reasons why the outsourced function is considered critical or important or not;

h) In the case of outsourcing to a cloud service provider, the cloud service and deployment models, i.e. public/private/hybrid/community, and the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored;

i) The date of the most recent assessment of the criticality or importance of the outsourced function.

In addition, the register should include for all existing and future outsourcing arrangements, the following information which the Central Bank deems necessary to assist in the effective monitoring and management of outsourcing risk:

General Information:

j) Total number of outsourced service arrangements in place;

k) Total number of "critical or important" outsourced arrangements in place;

l) Total number of arrangements with CSPs;

m) Confirmation that the firm has an Outsourcing Risk Management Framework in place;

n) Confirmation that the firm has an Outsourcing Policy in place;

o) Confirmation that the Outsourcing Policy is approved by the Board or equivalent;

p) Details of provision by the firm of outsourcing service(s) to other regulated firms.

q) Confirmation that Contracts / Written Agreements are supported by SLAs.

Finally, for the outsourcing of critical or important functions, the register should include at least the following additional information:

r) The firms within the scope of the prudential consolidation that make use of the outsourcing (i.e. the details of all of the firms / subsidiaries within a group using the service);

s) Whether or not the service provider or sub-service provider is part of the group or is owned by firms within the group;

t) The date/s of the most recent due diligence and risk assessments conducted including those involving services provided by sub-outsourcing providers and a brief summary of the main results;

u) The individual or decision-making body (e.g. the management body) in the institution or the payment institution that approved the outsourcing arrangement;

v) The governing law of the outsourcing agreement;

w) The dates of the most recent and next scheduled audits and reviews, where applicable - (to include reviews conducted by the regulated firms itself, its internal audit function and/or any independent third party reviews);

x) Where applicable, the names and details of any sub-contractors to which material parts of a critical or important function are sub-outsourced, including the country where the sub-contractors are registered, where the service will be performed and, if applicable, the location (i.e. country or region) where the data will be stored;

y) An outcome of the assessment of the service provider's substitutability (as easy, difficult or impossible), the possibility of reintegrating a critical or important function into the institution or the payment institution or the impact of discontinuing the critical or important function;

z) Identification of alternative service providers in line with point above;

aa) Whether the outsourced critical or important function supports business operations that are time-critical;

bb) Confirmation and latest dates of the testing of business continuity plans and exit strategies;

cc) Confirmation and dates of testing of OSPs business continuity plans;

dd) The estimated annual budget cost

ee) A record of terminated arrangements for an appropriate retention period.

10.2.1 Additional Information

Further to the information recorded within the register, the Central Bank may ask firms for additional information, in particular for critical or important outsourcing arrangements, such as:

- the detailed risk analysis and or the details and outcome of due diligence performed;
- the exit strategy for use if the outsourcing arrangement is terminated by either party or if there is disruption to the provision of the services; and
- the resources and measures in place to adequately monitor the outsourced activities.

Notes: In addition to the information set out above, the Central Bank may require regulated firms to provide detailed information on any outsourcing arrangement, even if the function concerned is not considered critical or important.

The submission of the data contained in the Registers (Databases) of firms will be by way of a periodic Regulatory Return. The frequency and timing of such returns will be specified to sectors by way of an Industry Letter.

Appendix 1 - Existing Sectoral Legislation, Regulations and Guidance

It is important that regulated firms consider this Guidance as supplemental to existing sectoral regulations and guidance on outsourcing and other related topics for their sector. It is a regulated firm's responsibility to ensure that it is compliant with all of the relevant laws, regulations and guidelines in force, including those applicable to outsourcing. Depending on the sector, these include (as of the publication of this Guidance):

Relevant Regulation, Guidance and Reports
Legislation
The Central Bank Reform Act 2010
Companies Act 2014
Regulation and Guidance - Markets
European Communities (Undertakings for Collective Investment in Transferable Securities) Regulations 2011 – S.1. No 352/2011.
European Union (Alternative Investment Fund Managers) Regulations – S.I. No. 257/2013, S.I. No. 379/2014
Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive
European Union (Undertakings for Collective Investment in Transferable Securities) (Amendment) Regulations 2016
European Union (Markets in Financial Instruments) Regulations 2017 – S.I. No. 375/2017.
Central Bank (Supervision and Enforcement) Act 2013 (Section 48(1)) (Undertakings for Collective Investment in Transferable Securities) Regulations - S.I. No. 420 of 2015, S.I. No 307 of 2016, S.I. No. 344 of 2017
Central Bank of Ireland AIF Rulebook
Central Bank (Supervision and Enforcement) Act 2013 (Section 48(1)) (Investment Firms) Regulations 2017 – S.I. No 604/2017.
Central Bank of Ireland Fund Administrators Guidance 2017
Central Bank of Ireland Fund Management Companies - Guidance 2016
Central Bank of Ireland Investment Firms Questions and Answers 5th Edition 2018
European Securities and Markets Authority ESMA 50-157-2403 Guidelines on Outsourcing to Cloud Service Providers
IOSCO Outsourcing Principles
Banking & Payments
European Banking Authority Guidelines on Internal Governance under Directive 2013/36/EU 2017
European Banking Authority Guidelines on Outsourcing Arrangements 2019 (EBA/GL/2019/02)
Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk 2011
European Banking Authority Guidelines on ICT and security risk management (EBA/GL/2019/04)
European Union (Payment Services) Regulations 2018

Insurance
European Union (Insurance and Reinsurance) Regulations 2015 (Solvency II Regulations)
European Insurance and Occupational Pensions Authority Guidelines on Systems of Governance 2016: GLs 14, 60, 62, 63, 64, 68
EIOPA Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002)
EIOPA Guidelines on ICT Security and Governance EIOPA-BoS-20/600
Information Security – IT & Cybersecurity
Central Bank of Ireland Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks 2016
Credit Unions
Credit Union Act 1997
Central Bank of Ireland Credit Union Handbook
Central Bank of Ireland Fitness & Probity Standards for Credit Unions
Central Bank of Ireland Guidance on Fitness & Probity for Credit Unions
Consumer Protection
Central Bank of Ireland Consumer Protection Code 2012
Fitness & Probity
Central Bank of Ireland Guidance on Fitness and Probity Standards 2018
Central Bank of Ireland Fitness and Probity Standards 2014
Anti-Money laundering
Anti-Money Laundering and Countering the Financing of Terrorism Guidelines for the Financial Sector Central Bank of Ireland - September 2019
Central Bank of Ireland Report on Anti-Money Laundering/Countering the Financing of Terrorism and Financial Sanctions Compliance - Life Insurance Sector 2016, Irish Funds Sector 2015, Banking Sector 2015
Other
Financial Stability Board Principles for an Effective Risk Appetite Framework 2013

Appendix 2 - Definitions and Criteria for Critical or Important Functions

General Note:

This Appendix 2 has been included for ease of reference, by firms, to relevant sectoral regulations and guidelines (applicable on a sectoral basis as at time of publication of this guidance) dealing with criteria relating to "critical or important".

The Central Bank has not included prescriptive definition of what constitutes 'critical or important' outsourcing arrangements, but rather (in line with other relevant guidelines) has suggested factors to be considered when determining if an activity/service is critical or important. The Central Bank does not feel it is appropriate to outline a list of critical or important activities/services, given that the financial service landscape is continually evolving and the use of new business models and technologies is ever changing. Rather a set of factors/criteria to be considered, which can be assessed against at a point in time and as part of a regular review cycle is proposed. Firms are expected to take a risk-based approach in their assessment of criticality and importance, bearing in mind the principle of proportionality.

Extracts from EBA/GL/2019/02 Guidelines on Outsourcing - Critical or Important functions – Criteria for Defining[31]

The Central Bank expects that each regulated firm will utilise, at a minimum, the following guidance in its determination of the applicability of defining an outsourcing arrangement as critical or important. The firm may choose to add other considerations to its assessment and if it does, so these should be documented in the firms outsourcing policy.

Regulated firms 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, Regulation (EU) No 575/2013, Directive 2014/65/EU, Directive (EU) 2015/2366 and Directive 2009/110/EC and their regulatory obligations;
    - their financial performance and or resilience (assets, capital, funding and liquidity); or
    - operational resilience including the soundness or continuity of their banking and payment services, insurance services and other activities;
    - impair financial stability

[31] The wording 'critical or important function', as in EBA/GL/2019/02, is based on the wording used under Directive 2014/65/EU (MiFID II) and Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II and is used only for the purpose of outsourcing; it is not related to the definition of 'critical functions' for the purpose of the recovery and resolution framework as defined under Article 2(1) (35) of Directive 2014/59/EU (BRRD).

- 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;

- 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 EBA/GL/2019/02

In the case of regulated firms, particular attention should be given to the assessment of the criticality or importance of functions if the outsourcing concerns functions related to core business lines and critical functions as defined in Article 2(1) (35) and 2(1) (36) of Directive 2014/59/EU36 and identified by institutions (firms) using the criteria set out in Articles 6 and 7 of Commission Delegated Regulation (EU) 2016/778.37. Functions that are necessary to perform activities of core business lines or critical functions should be considered as critical or important functions for the purpose of the EBA Guidelines, unless the institution's (firms) 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 operational continuity of the core business line or critical function.

When assessing whether an outsourcing arrangement relates to a function that is critical or important, regulated firms should take into account, together with the outcome of the risk assessment outlined in Section 12.2, of EBA/GL/2019/02 at least the following factors:

- whether the outsourcing arrangement is directly connected to the provision of banking activities or payment or insurance services for which they are authorised;

- the potential impact of any disruption to the outsourced function or failure of the OSP/CSP to provide the service at the agreed service levels on a continuous basis on their:
    - short- and long-term financial resilience and viability, including, if applicable, its assets, capital, costs, funding, liquidity, profits and losses;

    - business continuity and operational resilience;

    - operational risk, including conduct, information and communication technology (ICT) and legal risks;

    - reputational risks;

    - where applicable, recovery and resolution planning, resolvability and operational continuity in an early intervention, recovery or resolution situation;

- the potential impact of the outsourcing arrangement on their ability to:

    - identify, monitor and manage all risks;

- comply with all legal and regulatory requirements including GDPR or other applicable Data Protection legislation ;

- conduct appropriate audits regarding the outsourced function;

- the potential impact on the services provided to its counterparties, customers/clients and or policy-holders;

- all outsourcing arrangements, the regulated firm's aggregated exposure to the same OSP/CSP and the potential cumulative impact of outsourcing arrangements in the same business area;

- the size and complexity of any business area affected;

- the possibility that the proposed outsourcing arrangement might be scaled up without replacing or revising the underlying agreement;

- capability for early intervention, recovery and resolution planning and resolvability;

- the ability to transfer the proposed outsourcing arrangement to another service provider, if necessary or desirable, both contractually and in practice, including the estimated risks, impediments to business continuity, costs and time frame for doing so ('substitutability') in a stressed or non-stressed scenario;

- the ability to reintegrate the outsourced function into the institution or payment institution, if necessary or desirable;

- the protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the institution or payment institution and its clients, including but not limited to compliance with Regulation (EU) 2016/67939 .

Extracts from Solvency II and EIOPA Guidelines

EIOPA's SOG GLs – GL 60 outlines that an undertaking determines whether an outsourcing arrangement is critical or important function or activity, on the basis of whether the function or activity is essential to the operation of the undertaking as it would be unable to deliver its services to policyholders without the function or activity i.e. as in;

- ability to provide an appropriate degree of protection for those who are or may become policyholders in line with the CBI's statutory objectives; and
- requirement not to undermine the 'continuous and satisfactory service to policy holders' in line with Article 49(2) (c) of Solvency II.

Examples of critical or important functions or activities include:

- the design and pricing of insurance products;
- the investment of assets or portfolio management;
- claims handling;
- the provision of regular or constant compliance, internal audit, accounting, risk management or actuarial support;
- the provision of data storage;
- the provision of on-going, day-to-day systems maintenance or support;

- the ORSA process.

Extracts from Markets related Regulation and Guidelines

The EBA/GL/2019/02 definition is based on the Directive 2014/65/EU (MiFID II) and Articles 30-31 of the Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II.

The use of the term 'critical or important functions' is based on the wording of MiFID II and the Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II. It is used only for the purpose of identifying 'critical or important functions' under outsourcing arrangements to which a specific set of requirements apply. Commission Delegated Regulation (EU) 2017/565 specifies, under Article 30, that 'an operational function shall be regarded as critical or important 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 Directive 2014/65/EU, or its financial performance, or the soundness or the continuity of its investment services and activities'.

The same approach exists under Directive 2009/138/EC12 (Solvency II), while, in the context of outsourcing, the PSD2 uses 'important function' for the purpose of identifying functions under outsourcing arrangements for which specific requirements apply. Therefore, to embrace all existing legislation and to ensure a level playing field for credit institutions, investment firms, payment institutions and electronic money institutions, the wording used under MiFID II is used within the EBA Outsourcing Guidelines.

Investment Firms Regulation SI 604 of 2017
The regulation sets out the requirements for outsourcing arrangements but does not distinguish between critical or important or not.

Fund Administration Outsourcing Guidance
The Guidance for Fund Administrators (June 2017) refers to the concept of "materiality" but does not define it. However, the guidance covers many of the criteria listed above as considerations for risk assessing proposed arrangements.

Credit Unions

The Credit Union Act (76J 11a) definition of "material" business activity equates to key aspects of the EBA's GL/2019/02 "critical or important".

Ref Credit Union Act and Handbook
11b) In this subsection and subsection (12) 'material business activity' means an activity where a defect or failure in its performance would materially impair-

(i) the continuing compliance with the conditions and obligations of its registration or its other obligations under the financial services legislation,

(ii) its financial performance,

(iii) the soundness or continuity of its financial performance, or

(iv) the soundness or continuity of its business.

Appendix 3 - Sample for Guidance on Content and Completion of Register/Database and CBI Regulatory Return[32]

Key Elements	EBA Guidelines Reference	Guidance for Firms
All Outsourcing Agreements		
	Para 54(a) A reference number for each outsourcing arrangement.	Suggest form of unique identifier
	Para 54(b) – the start date and, as applicable, - the next contract renewal date, - the end date – and/or notice periods for the service provider and for the institution. For Fund Administrators the date when permission granted and the "Go Live" date	**Report dates in a YYYYMMDD format** Start Date End Date Notice Period (In months) Contract Renewal Date (Blank Fields will be interpreted as Not Applicable)
	Para 54(c) A brief description of the outsourced function (See EBA Spreadsheet for sample list of functions and activities), including the data that are outsourced and whether or not personal data (e.g. by providing a Yes or No in a separate data field) have been transferred or if their processing is outsourced to a service provider. The Guidance on Outsourcing for Fund Administrators requires: Details of Final NAV Model and the Funds which utilise the arrangement	Firms to describe the function in 250 characters. **Personal Data** - Y/N
	Para 54(d) A category assigned by the institution that reflects the nature of the function as described above (e.g. information technology (IT), control function), which should facilitate the identification of different types of arrangements.	**Category** Reference: For consistency - See EBA Register Template - Spreadsheet
	Para 54(e) – the name of the service provider – the corporate registration number – the legal entity identifier (where available) – the registered address – other relevant contact details, and – the name of its parent company (if any).	**Use a standard legal entity identifier.** Possibilities include: LEI **The category of the outsource service provider** (OSP) should be defined i.e. : • TPV

[32] The content of the Template is based on the requirements for EBA Guidelines on Outsourcing /GL/2019/02, EIOPA Cloud Outsourcing Guidelines and ESMA 50-157-2403 Guidelines for Outsourcing to Cloud Service Providers.

	Is the OSP a regulated entity Y/N - If Y then who is the Regulator	• Sub-outsourcer • Intragroup • Fintech Firm • Partnership Regulated Entity Y/N if Yes Name of Regulator
	Para 54(f) The town/city and country or countries where the service is to be performed, including the location (i.e. country or region) of where the data is located. Consider: Is there sensitive business or customer data at risk? Is the data being offshored outside the EU/EEA area?	**If the answer is Yes to either question then details should be provided**. Locations should specify Country[33] and Town/City where service is performed and where data is stored and processed. **Service Performed:** Countries should be specified by using naming convention i.e., ISO 3166-1 alpha-2 code. **Data Stored and Processed:** Countries should be specified by using naming convention i.e., ISO 3166-1 alpha-2 code.

	Para 54(g) – Is the outsourced function 'critical' or 'important'? Include a brief summary of the reasons/criteria why it's considered critical or important or not.	**Critical or Important** - Y/N Firms to describe why function/service is deemed critical or important in 250 characters - Referencing EBA or other regulatory criteria.
	Para 54(h) – in the case of outsourcing to a cloud service provider, the cloud service and deployment models, i.e. public/private/hybrid/community, - the specific nature of the data to be held – and the locations (i.e. countries or regions) where such data will be stored.	**Cloud Services** **Deployment Model**: • Public • Private • Hybrid • Community **Location of Data**: Countries should be specified by using naming convention i.e., ISO 3166-1 alpha-2 code. **Nature of Data**: Firms to summarise the specific nature of the data being held in 250 characters.

[33] ISO 3166-1 alpha 2 code - The purpose of ISO 3166 is to define internationally recognized codes of letters and/or numbers that we can use when we refer to countries and their subdivisions. This should be used by firms to ensure a consistent naming convention throughout the Register.
The code and listings are available at: https://www.iso.org/iso-3166-country-codes.html

	Para 54(i) the date of the most recent assessment of the criticality or importance of the outsourced function.	**Report dates in a YYYYMMDD format** **Date of Assessment**:
Critical or Important Outsourcing Arrangements		
	Para 55(a) the firms within the scope of the prudential consolidation, where applicable, that make use of the outsourcing.	**Link to firms' FRN** or other identifier if based outside Ireland.
	Para 55(b) whether or not the service provider or sub-service provider is part of the group or is owned by firms within the group.	Y/N **Relationship details**: Firms to describe the relationship in 250 characters.
	Para 55(c) the dates of the most recent due diligence and risk assessments conducted including those involving services provided by sub-outsourcing providers and a brief summary of the main results.	**Report dates in a YYYYMMDD format** **Due Diligence Date:** **Risk Assessment Date:** Firms to summarise due diligence / risk assessment results in 250 characters.
	Para 55(d) the individual or decision-making body (e.g. the management body) in the institution that approved the outsourcing arrangement.	
	Para 55(e) the governing law of the outsourcing agreement.	
	Para 55(f) the dates of the most recent and next scheduled audits, where applicable (to include reviews conducted by the regulated firm itself, its internal audit function and/or any independent third party reviews).	**Report dates in a YYYYMMDD format.**
	Para 55(g) - the names of any sub-contractors to which material parts of a critical or important function are sub-outsourced, including: - the country where the sub-contractors are registered, - where the service will be performed, and - the location (i.e. country or region) where the data will be stored.	**Use a standard legal entity identifier.** Possibilities include: LEI Use standard country names and internationally recognised three letter identifiers. Country of registration: Country where service is performed:

		Country where data is stored:
	Para 55(h) - the outcome of the assessment of the service provider's substitutability (e.g. easy, difficult or impossible) - the possibility of reintegrating a critical or important function into the institution OR - the impact of discontinuing the critical or important function.	Firm to name possible substitute. or Firms to summarise in 250 characters why 'difficult' or 'impossible' if chosen. **Reintegration possible** Y/N Firms to describe in 250 characters the impact of discontinuing the function.
	Para 55(i) identification of alternative service providers in line with the point above.	**Legal entity name should be used consistently throughout response.**
	Para 55(j) whether the outsourced 'critical or important function' supports business operations that are time-critical. 'Time-critical' needs defining in Firm's Outsourcing Policy.	**Tie the definition of 'Time Critical' to Impact Tolerances.** – These should be referenced in the firms Outsourcing Policy
	Para 55(k) the estimated annual budget cost.	
	A record of terminated arrangements for an appropriate retention period.	Free text list of most recent terminations with dates Report dates in a YYYYMMDD format.
	Confirmation and Dates of testing of firm's business continuity plans. The testing of these plans needs to be integrated into/coordinated with the firm's BCM arrangements. The status of the testing of these arrangements should be logged and tracked in the register/database	**Report dates in a YYYYMMDD format.**
	Confirmation and Dates of testing of OSPs business continuity plans	**Report dates in a YYYYMMDD format.**
	Confirmation and Dates of testing of firm's Exit Strategies. The review and testing of Exit Strategies should be documented in the database / register	**Report dates in a YYYYMMDD format.** **Review of Exit Strategy** Date: **Testing of Exit Strategy** Date:

Additional Data required by the CBI to be retained and documented[34] - All Outsourcing Arrangements	**General Information**	**Guidance for Firms**
	Total number of outsourced service arrangements in place	**Number** This should include all critical or important arrangements and non-critical or important whether with external Third Party Vendors (TPVs) or Intragroup arrangements
	Total number of "critical and or important" outsourced arrangements in place.	**Number**
	Total number of arrangements with Cloud Service Providers (CSPs)	**Number**
	Does the firm have an Outsourcing Risk Management Framework in place?	Y/N
	Does the firm have an Outsourcing Policy in place?	Y/N
	Is the Outsourcing Policy approved by the Board?	Y/N
	Does the firm provide outsourcing services to other regulated firms?[35]	Y/N If yes then provide a brief description, in 250 characters, of the services provided and to whom.
	Are Contracts / Written Agreements supported by SLAs?	Y/N

[34] Suggested additional data to be retained in the firm's register/database in order to complete the CBI Regulatory Return.
[35] This is to assist CBI understand cross-firm, cross-sector and cross-industry concentrations.

Appendix 4 - Definitions

The following definitions have been included by the Central Bank to provide additional clarity on terms or concepts used in this Guidance.

Board, Senior Management and the Management Body – these are terms used to address the body, bodies and/or individuals that are appointed in accordance with national law, which are empowered to set the regulated firm's strategy, objectives and overall direction, and which oversee and monitor management decision-making. It includes the persons who effectively direct the business of the regulated firms and the directors and persons responsible for the management of the regulated firm. It is acknowledged that some smaller, less complex firms may not have a board of directors. In these cases, where the term 'board and senior management' is used, it is intended to address the relevant management bodies or structures of these regulated firms.

Vendor lock-in - means a situation where a regulated firm finds that due to the unavailability of alternative suitable supplier of an outsource service it is in essence "locked in" to the existing arrangement

Cloud computing or cloud – means a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources (for example servers, operating systems, networks, software, applications, and storage equipment) with self-service provisioning, and administration on-demand.

Cloud Deployment Model – means the way in which cloud may be organised based on the control and sharing of physical or virtual resources. Cloud deployment models include community[36], hybrid[37], private[38] and public[39] clouds.

Cloud Services – means services provided using cloud computing.

Cloud Service Provider (CSP) – is as per the definition of OSP above, but relates specifically to the provision of outsourced cloud services. The term CSP may be used from time to time in this

[36] A cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection;

[37] A cloud deployment model that uses at least two different cloud deployment models;

[38] A cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer;

[39] A cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider.

Guidance to refer to cloud specific issues and requirements. However, it is important to note that where the term OSP is used more broadly throughout the guidance, it includes CSPs.

Concentration risk – means the risk of loss or service disruption arising from a lack of diversification of OSPs. This can arise in the case of an individual firm, who relies on a single or small number of OSPs for the provision of their critical or important functions. It can also arise on a sectoral or cross-sectoral basis.

Critical or important functions – means any function that is considered critical or important as set out in Part B Section 1 above.

Function – means any processes, services or activities.

Outsourcing - means an arrangement of any form between a regulated firm and an outsourced service provider (OSP) by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the regulated firm itself, even if the regulated firm has not performed that function itself in the past.

Outsourced Service Provider (OSP) – means a third-party entity that is undertaking an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement. This term is used in this Guidance to refer to both external third party service providers and intra/inter group service providers (See also CSP below).

Sub-outsourcing – means a situation where the service provider under an outsourcing arrangement further transfers the performance of an outsourced function, or parts of a function, to another service provider. Sub-outsourcing is a feature of both external third party service providers and intra/inter group service providers. Sub-outsourcing is often referred to as chain-outsourcing and service providers in the chain other than the primary OSP are referred to as sub-contractors.

T: +353 (0)1 224 6000
E: outsourcingfeedback@centralbank.ie
www.centralbank.ie

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem