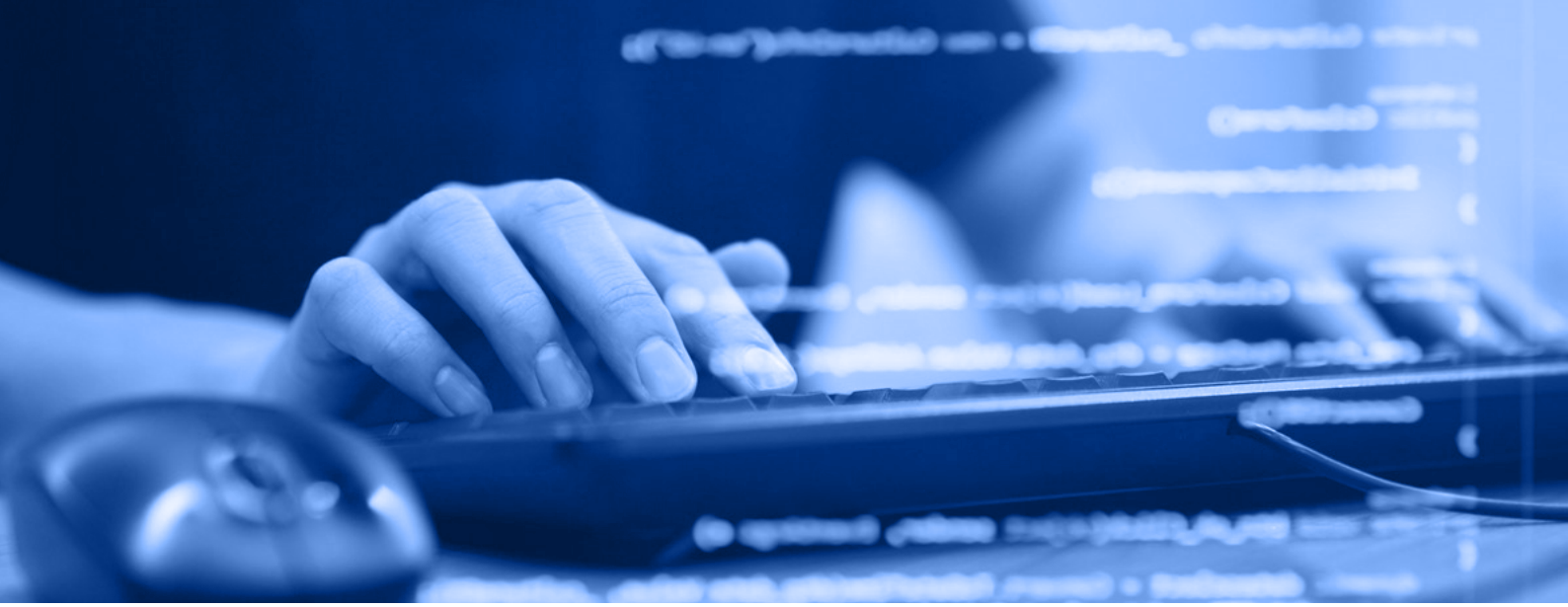
Matheson

May 2024

Outsourcing Toolkit

CONTENTS Page No



1 Introduction

1.1 The Central Bank of Ireland (the "**Central Bank**") has observed an increasing reliance by regulated financial service providers on outsourced service providers ("**OSPs**") in recent years. In light of the evolving financial services landscape, growing international focus on outsourcing and increasing concerns in relation to outsourcing governance and risk management, the Central Bank has undertaken a significant programme of work in relation to outsourcing arrangements. This has included the publication of the paper 'Outsourcing – Findings and Issues for Discussion' in November 2018[1] and the hosting of an industry outsourcing conference in April 2019 and in February 2021 the "Consultation Paper 138 Cross-Industry Guidance on Outsourcing" ("**CP138**") and draft Cross-Industry Guidance on Outsourcing (the "**Draft Guidance**"). The Draft Guidance was proposed to support and complement the existing sectoral legislation, regulations and guidelines on outsourcing and the consultation process was open until 26 July 2021. On 21 December 2021, the Central Bank published the final Cross-Industry Guidance on Outsourcing (the "**Guidance**").

We hope you find the Outsourcing Toolkit useful and that it becomes your go to resource for outsourcing matters going forward. Should you have any queries in respect of the materials included in The Matheson Outsourcing Toolkit, please do not hesitate to contact any of the Outsourcing team.

1 Outsourcing – Findings and Issues for Discussion November 2018.

Contacts

Darren Maher
Partner | Head of Financial Institutions Group
T +353 1 232 2398
E darren.maher@matheson.com

Joe Beashel
Partner | Financial Institutions Group
T +353 1 232 2101
E joe.beashel@matheson.com

Gráinne Callanan
Partner | Financial Institutions Group
T +353 1 232 8211
E grainne.callanan@matheson.com

Niamh Mulholland
Partner | Financial Institutions Group
T +353 1 232 2061
E niamh.mulholland@matheson.com

Caroline Kearns
Partner | Financial Istitutions Group
T +353 1 232 2421
E caroline.kearns@matheson.com

Elaine Long
Partner | Financial Institutions Group
T +353 1 232 2694
E elaine.long@matheson.com

Tara Doyle
Partner | Asset Management and Investment Funds Group
T +353 1 232 2221
E tara.doyle@matheson.com

Dualta Counihan
Partner | Asset Management and Investment Funds Group
T +353 1 232 2451
E dualta.counihan@matheson.com

Philip Lovegrove
Partner | Asset Management Investment Funds Group
T +353 1 232 2538
E philip.lovegrove@matheson.com

Shay Lydon
Partner | Asset Management and Investment Funds Group
T +353 1 232 2735
E shay.lydon@matheson.com

Michelle Ridge
Partner | Asset Management and Investment Funds Group
T +353 1 232 2758
E michelle.ridge@matheson.com

Barry O'Connor
Partner | Asset Management and Investment Funds Group
T +353 1 232 2488
E barry.oconnor@matheson.com

Anne Marie Bohan
Partner | Head of Technology and Innovation Group
T +353 1 232 2212
E anne-marie.bohan@matheson.com

Carlo Salizzo
Partner | Technology and Innovation Group
T +353 232 2011
E carlo.salizzo@matheson.com

Karen Reynolds
Partner | Commercial Litigation and Dispute Resolution Department
T +353 1 232 2759
E karen.reynolds@matheson.com

Should you require further information in relation to the material contained in this Toolkit, please get in touch with a member of the team at the contact information above or your usual Matheson contact. Full details of Matheson's Financial Institutions group together with further updates, articles and briefing notes written by members of these teams, can be accessed at www.matheson.com

2 Regulatory Concerns

2.1 The Central Bank notes in CP138 that the financial service landscape is continually evolving and that outsourcing is increasingly been utilised by financial service providers as a key strategic tool to respond to and manage the changing landscape. There are a number of keys risks which the Central Bank has identified with regards to outsourcing which include the following:

a. the increasing role of technology reflected in the recent rapid growth in the number of fintech and regtech firms, and the use of cloud service providers ("**CSPs**") by firms[2]. The Central Bank expects firms to implement a robust governance framework to manage the specific risks associated with outsourcing of their critical or important services to CSPs;

b. concentration Risk - The Central Bank has specifically highlighted that the increasing use of outsourcing arrangements, particularly in respect of cloud outsourcing, is resulting in increased levels of concentration risk. Firms should be aware that discussions are ongoing at EU and international levels regarding systemic concentration risk and the potential implications on financial stability and that the outcome of these discussions could result in changes to the regulatory framework over time[3];

c. suboutsourcing Risk - The Central Bank has emphasised that it is particularly important to ensure that sub-outsourcing does not impair the Firms visibility and a regulator's supervisibility of activities being performed[4]. The Central Bank has also emphasised that 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[5]. Therefore, the board and senior management must ensure that they understand where the relevant regulated financial service provider sits in terms of priority within the group structure and that any conflicts of interest are identified and properly managed. In particular in relation to intragroup outsourcing arrangements, the Central Bank notes that it expects firms to "*apply the same rigor when conducting intragroup risk assessments as for third party OSP assessments*"; and

d. offshoring Risk – Visibility and supervisibility risk is 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.

2 Section 3.2, Consultation Paper 138 for Cross-Industry Guidance on Outsourcing.

3 Section 2, Cross-Industry Guidance on Outsourcing December 2021.

4 Section 2, Cross-Industry Guidance on Outsourcing December 2021.

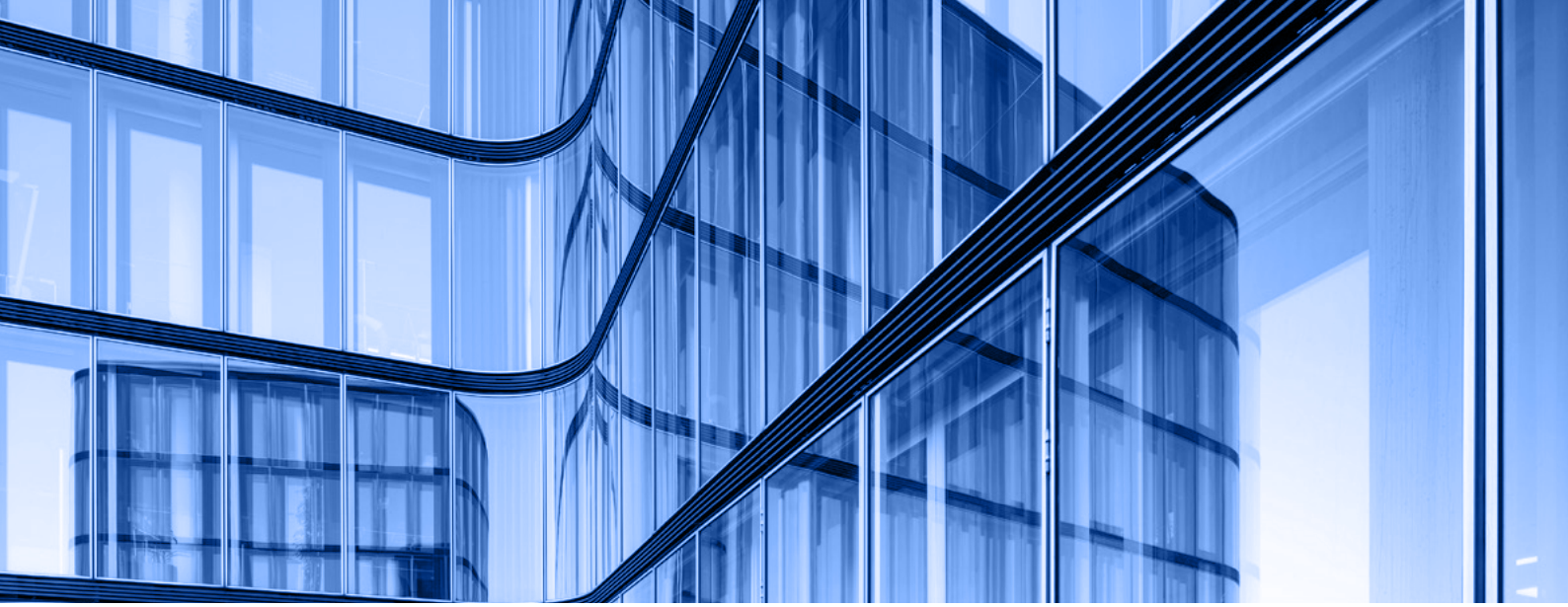
5 Section 2, Cross-Industry Guidance on Outsourcing December 2021.

2.2 The Guidance sets out the Central Bank's expectations in relation to managing the aforementioned risks.

2.3 The Central Bank has continuously emphasised that responsibility and accountability for the effective oversight for all regulated activities, whether outsourced or not, ultimately rests with the board and senior management. This is strongly reiterated in CP138 and the Guidance. Boards and senior management of regulated financial service providers must be cognisant of the fact that when entering into outsourcing arrangements they are creating a dependency on a third party, or a chain of such parties. This has the potential to influence the operational resilience of firms, the quality and service of products delivered to consumers and the operation of the market[6]. As such, boards and senior management of regulated financial service providers must ensure that an appropriate risk and governance framework is in place to enable a comprehensive view and oversight of the outsourcing universe and mitigate potential risks of financial instability and consumer detriment.

2.4 The purpose of this toolkit (the "**Toolkit**") is to provide regulated financial service providers ("**Firms**") with checklists as a resource and a reference point to be used throughout the life-cycle of an outsourcing arrangement, which may assist in meeting the Central Bank's expectations as set out in the Guidance in relation to outsourcing. It is important to note that this Tooklit is not intended to identify a specific Firm's outsourcing obligations. Firms should consider the Toolkit in conjunction with any sectoral laws, regulations and guidance for its respective sector.

6 Section 1.4, Consultation Paper 138 for Cross-Industry Guidance on Outsourcing.



3 Applicable Legal and Regulatory Requirements

3.1 The Guidance lists the sector specific outsourcing laws, regulations and guidelines applicable to firms[7]. While the primary legislation specific to each sector does impose obligations on Firms in relation to outsourcing, which of course Firms should be cognisant of, the sectoral guidelines are often more prescriptive in terms of what steps Firms should take to ensure that they are in compliance with their outsourcing obligations. Accordingly, we have collated the guidance which is relevant to Firms below and provided links to the relevant guidance for ease or reference (This was accurate as at the date of publication).

GUIDANCE FOR FIRMS
Investment Firms
■ 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)
Insurance
■ 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

7 Appendix 1, Cross-Industry Guidance on Outsourcing December 2021

Information Security – IT & Cybersecurity

- Central Bank of Ireland Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks 2016

Credit Unions

- 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

Investment Funds[8]

- Central Bank of Ireland AIF Rulebook
- Central Bank of Ireland Fund Administrators Guidance 2017
- Central Bank of Ireland Fund Management Companies Guidance 2016

Other

- Financial Stability Principles for an Effective Risk Appetite Framework 2013
- Financial Stability Board Discussion Paper - Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships

8 The Guidance applies in a proportionate manner to fund service providers associated with the operation of the fund and not to the investment fund itself. The board of directors of an externally managed investment fund should, however, ensure that it supports the ability of the fund management company to comply with all regulatory obligations, including the Guidance. The Central Bank has confirmed that the Guidance applies to fund depositaries and custody arrangements and will apply to outsourcing arrangements involving critical financial market infrastructure in a manner consistent with the Firm's nature, scale and complexity.

4 Checklists

4.1 The checklists below (the "**Checklists**") set out, at a high level, the minimum supervisory expectations placed upon Firms where outsourcing critical or important operational functions. We have provided 10 "key" checklists which are relevant throughout the different stages of an outsourcing arrangement:

(i) Considerations for the board and senior management prior to entering into an outsourcing arrangement;

(ii) General requirements that Firms must consider prior to outsourcing a critical or important function(s);

(iii) Key risks that Firms should consider when completing an initial risk analysis in respect of an outsourcing arrangement;

(iv) What due diligence should be undertaken;

(v) What are the reporting requirements to the Central Bank in respect of critical or important function(s);

(vi) What are the requirements for the written outsourcing agreement;

(vii) What is the outsourcing register;

(viii) How to ensure that proper and effective oversight of outsourcing arrangements is maintained by the Firm;

(ix) What are the key data management measures; and

(x) Exit strategy considerations.

Outsourcing Checklists

1 Considerations for the board and senior management prior to entering into an outsourcing arrangement

No	Requirement	Guidance	✓
The general responsibilities of board and senior management in respect of outsourcing arrangements are set out below:			
1.	**Ultimate Responsibility**	The board and senior management of Firms are ultimately accountable for all activities undertaken by the Firm. This includes responsibility for the effective oversight and management of outsourcing risk within their business	☐
2.	**Board Responsibility – Effective Governance and Oversight**	In ensuring effective oversight, the board and senior management should: ▪ ensure that the governance and risk management of their outsourcing frameworks are appropriate and operating effectively in line with supervisory expectations and relevant sectoral legislation, regulation and guidelines; ▪ have appropriate and effective governance and internal controls; ▪ implement an appropriate framework to provide a comprehensive view of the Firm's outsourcing universe to the board; ▪ ensure that outsourcing does not impede the Firm's ability to meet its authorisation conditions; ▪ maintain at all times sufficient substance to ensure their Firms do not become 'empty shells' or letter-box entities; and ▪ ensure that outsourcing arrangements do not create impediments to the resolvability of the Firm.	☐
3.	**Outsourcing Framework**	The outsourcing framework should include: ▪ a documented outsourcing strategy, which is aligned to the Firm's business strategy, business model, risk appetite and risk management framework; ▪ definitions of critical or important functions in the context of the Firm's business; ▪ a defined methodology for determining the 'criticality or importance'[9] of service; ▪ a comprehensive outsourcing policy; ▪ an outsourcing register; and ▪ defined reporting requirements to ensure the provision of timely and appropriate management information ("**MI**") to the board,	☐
4.	**Skills and Knowledge**	Ensure that appropriate skills and knowledge are maintained within the Firm to effectively oversee outsourcing arrangements from inception to conclusion.	☐
5.	**Designated Responsibility within the Firm**	Assign responsibility for oversight of outsourcing risk / outsourcing arrangements to an appropriately designated individual, function and / or committee which should be directly accountable to the board.	☐

9 In conjunction, with Firm specific legislation and regulation, the Central Bank expects Firms to have regard to the following definition 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.*'

2 Guidance Prior to Outsourcing

No	Requirement	Guidance	✓
The general responsibilities of board and senior management in respect of outsourcing arrangements are set out below:			
1.	**Assessment of Criticality or Importance of activity / service to be outsourced**	The Firm should conduct an assessment of criticality or importance of the services to be outsourced, prior to signing an outsourcing contract or written outsource agreement. This assessment should be conducted against the Firm's defined methodology for determining the 'criticality or importance' of a service which: ▪ clearly sets out the criteria / factors that form this determination / rationale; ▪ can be applied consistently and is in line with relevant sectoral regulations and guidance; ▪ considers the nature, scale and complexity of a Firm's business; and ▪ is assessed and approved by the board on a regular basis.	☐
2.	**Outsourcing and Delegation**	The Central Bank has noted that "delegation" and "outsourcing" are not considered different concepts[10]. In respect of the assessment of delegation arrangements, Firms should: ▪ apply the same standards to delegated arrangements as to other outsourcing arrangements; ▪ ensure appropriate governance / risk management measures are implemented for delegated arrangements; and ▪ evidence appropriate oversight of delegation arrangements and that the board has considered the risks associated with same.	☐
3.	**Outsourcing Strategy**	Firms should have a documented outsourcing strategy. In formulating this strategy, a Firm should at least consider the following areas: ▪ the extent of the outsourcing; ▪ the types of activities and functions that they will consider outsourcing; ▪ the risks to the Firm / the ability to evidence how risks will be managed and mitigated; ▪ the extent to which the Firm has the skills / capacity to exercise oversight of the outsourcing arrangements; ▪ in the context of information and communications technology ("**ICT**"), a Firm's capability to oversee and manage the cloud outsourcing arrangements; and ▪ whether the Firm's outsourcing strategy informs a board approved comprehensive outsourcing policy.	☐

10 Section 3(a), Cross-Industry Guidance on Outsourcing December 2021. In addition to stating that no difference should be inferred between "delegation" and "outsourcing", the Central Bank has confirmed that the Guidance applies to outsourcing arrangements involving critical financial market infrastructure, including clearing and settlement services provided by Central Securities Depositaries and Central Counterparties, in a manner consistent with the Firm's nature, scale and complexity. Fund depositaries are currently considering the proportionate and practical application of all aspects of the Guidance to these arrangements.

4.	**Outsourcing Policy – General**	Firms should have a documented firm-wide outsourcing policy, which is reviewed and approved by the board at least annually. The outsourcing policy should address at a minimum:
		▪ risk appetite in respect of outsourcing;
		▪ roles and responsibilities for the oversight and management of outsourcing risk, including:
		  ▪ the responsibilities of the board and its involvement in providing direction and decisions relating to outsourcing; and
		  ▪ the responsibilities of business lines and internal control functions with regard to outsourcing.
		▪ the process for approval of new outsourcing arrangements;
		▪ the requirement to establish contracts, written agreements and by service level agreements ("**SLAs**");
		▪ the Firm's policy with regard to sub-outsourcing and if this is permitted under contractual arrangements with OSPs;
		▪ the approach to identifying and addressing potential conflicts of interests;
		▪ the record keeping requirements in relation to outsourcing arrangements; and
		▪ any differences in the Firm's approach to the governance and management of:
		  ▪ critical or important outsourcing arrangements and other outsourcing arrangements;
		  ▪ outsourcing to regulated OSPs versus non-regulated OSPs;
		  ▪ outsourcing to an intra-group OSP versus external third party OSP; and
		  ▪ outsourcing to OSPs located within the EU / EEA and those located in third countries.
			☐

5.	**Outsourcing Policy – Risk Management Framework**	The Firm's outsourcing policy should provide details of the framework to enable operational oversight including: ▪ the frequency, approach and rationale underpinning regular review of the performance levels of OSPs; ▪ the notification procedures for changes to an outsourcing arrangement and responding to such notifications; ▪ the arrangements for independent review and audit; and ▪ the decision points and escalation routes for provision of MI to the board.	☐
6.	**Outsourcing Policy – Data Management**	The Firm's outsourcing policy should include the approach to safeguarding and maintaining the integrity of the Firm's data and systems as set out in a Firm's management strategy.	☐
7.	**Outsourcing Policy – Exit Strategy**	The Firm's outsourcing policy should document: ▪ the approach to business continuity arrangements in respect of outsourcing arrangements; ▪ the requirement for a documented exit strategy for each outsourcing arrangement deemed critical or important; and ▪ the termination processes, including consideration of unexpected termination of an outsourcing arrangement and contingency arrangements.	☐

8.	**Intragroup Arrangements**	When entering into an intragroup arrangement, the board and senior management must: ▪ apply the same rigor to intragroup outsource risk assessments as that applied to third party OSP assessments; ▪ be satisfied with the extent to which the Firm is in a position to exert sufficient influence on the group / or parent entity providing the service; ▪ be satisfied with the application of the appropriate level of prioritisation of any remediation of outsourced services, where service outages may impact the Firm and wider group; ▪ ensure that the resolution of any potential conflicts of interest is provided for in the governance arrangements; and ▪ assess if policies and procedures applied at group level are fit for purpose at the local Irish legal entity level and are in compliance with Irish legal and regulatory obligations.	☐
9.	**Outsourcing of Risk Management and Internal Control Functions**	In respect of the outsourcing of any part of their risk management or internal control functions, Firms must: ▪ consider the outsourcing risks of such functions and evidence that the board or senior management of the Firm are satisfied that there are no significant concerns about the internal control and governance framework; ▪ maintain adequate oversight of these functions; and ▪ apply due care and attention when considering and appointing the outsourcing of Pre-Approval Controlled Functions ("**PCFs**") and Controlled Functions ("**CFs**").	☐

10. Disaster Recovery and Business Continuity Management

When designing and implementing disaster recovery ("**DR**") and business continuity measures ("**BCM**") in respect of any critical or important outsourced arrangements, Firms should consider the following:

- consider DR / BCM of an OSP and ensure that service disruptions can be maintained within the impact tolerances and recovery time objectives of the firm as documented within its most recent business impact analysis;
- ensure that all governance arrangements reflect any implications of the outsourcing arrangement;
- document and implement business continuity plans ("**BCPs**") in relation to their critical and important outsourced functions and ensure that these plans are tested and updated on a regular basis;
- consider the need for the creation of periodic isolated "safe harbour" backup arrangements in respect of cloud outsourcing arrangements as part of their business continuity planning;
- ensure the OSP has a BCP in place;
- ensure that the outsourcing arrangement includes a requirement for the OSP to carry out testing of its own BCPs at least annually;
- ensure that they can participate in the OSPs BCP testing;
- conduct coordinated testing of these arrangements on a regular basis and report to both the Firm and the OSP;
- review reports on BCM and testing undertaken by the OSP and any relevant remediation arising as a result of this testing, as appropriate;
- take remedial action to address any deficiencies identified in the performance of the OSP;
- regularly review the appropriateness of their BCPs and resilience measures, particularly in the context of new and evolving technologies, trends and risks; and
- ensure that outsourcing arrangements are considered in the context of a Firm's recovery planning and resolution planning and that scenarios of financial distress are considered.

3 Initial Risk Analysis Prior to Outsourcing

No	Requirement	Guidance	✓
The key risks a Firm must consider prior to entering into an outsourcing arrangement are set out below:			
1.	**Risk Assessment and Monitoring**	A Firm must ensure that its risk management framework appropriately considers any outsourcing arrangements and that outsourcing risk is reflected in the Firms overarching risk register. The Firm must also document the controls to be put in place and ensure that these controls and the mechanism for monitoring their effectiveness, are reflected in the relevant outsourcing contracts and SLAs.	☐

2.	**Initial Risk Analysis**	When developing their outsourcing risk management framework and conducting outsourcing risk assessments, Firms should consider the following factors:
		▪ conduct comprehensive risk assessments prior to entering into an outsourcing arrangement;
		▪ ensure that outsourcing risk assessments consider specific risks associated with outsourcing including but not limited to:
		  ▪ sub-outsourcing risks;
		  ▪ sensitive data risks;
		  ▪ concentration risks, including over-dependence on a single or small number of OSPs which cannot easily be substituted;
		  ▪ offshoring risks;
		  ▪ step-in risk;
		  ▪ business continuity risks / threats to the Firms operational resilience through its dependence on OSPs.
		  ▪ legal, regulatory and reputational risks in respect of the outsourced services; and
		  ▪ any specific risks associated with cloud outsourcing.
			☐

3.	**Sub-Outsourcing Risk**	In order to effectively manage the risks associated with sub-outsourcing, the Firm should: ▪ determine its appetite for sub-outsourcing; ▪ ensure specific provisions relating to sub-outsourcing are included in contractual arrangements; ▪ ensure sub-outsourcing risks arising from intragroup arrangements are treated the same as external third party OSPs; ▪ monitor sub-outsourcing of critical or important functions, for exposure to concentration risks related to the sub-outsourced service providers; ▪ ensure that the OSP manages the activities of the sub-outsourced service provider in line with the outsourcing contract and relevant SLAs; ▪ apply an appropriate level of monitoring of the sub-outsourced service providers in line with their outsourcing risk assessment; and ▪ not agree to sub-outsourcing unless the sub-contractor agrees to comply with the relevant laws, regulatory requirements and contractual obligations and provide the Firm and the Central Bank the same contractual rights of access and audit as those granted by the primary OSP.	☐

4.	**Concentration Risk – General**	In an outsourcing context, concentration risk is the probability of loss arising from a lack of diversification[11] of OSPs. In order to monitor and manage this risk, Firms should regularly implement appropriate measures to manage: ▪ overall exposure and reliance on OSPs and sub-contractors; ▪ concentration risks or vendor lock-in at firm or group level, due to multiple arrangements with the same / closely connected service providers with OSPs where a substitutability issue exists; ▪ ensure that its risk management framework includes its approach to the management of concentration risk; ▪ ensure that its ability to negotiate and secure robust arrangements with such providers is not hindered; ▪ endeavour to secure satisfactory contractual terms from OSPs and reinforce them with appropriate SLAs; and ▪ include conditions in the outsourcing written agreement that require the prior approval of the outsourcing Firm to the possibility and modalities of sub-outsourcing.	☐
5.	**Concentration Risk – Risk Assessments**	In order to monitor and manage concentration risk, Firms should evaluate elements of concentration risk and consider the following: ▪ single firm concentration of multiple services at same OSP or intragroup service provider; ▪ lack of substitutability issue arising from single service provider in the marketplace; ▪ multiple number of Firms outsourcing to same OSP either on a sectoral or cross sectoral basis; ▪ concentration risk arising from chain outsourcing (sub-outsourcing / sub-contracting) arrangements; ▪ concentration risk arising from outsourcing to offshore jurisdictions; and ▪ contribution to systemic outsourcing concentration risk.	☐
6.	**Offshoring Risk**	Firms should evaluate the particular risks associated with countries to which they are planning to outsource activities and must document the assessment. Firms should give consideration and take steps to mitigate the following offshoring risks: ▪ regulatory environment; ▪ legal risk; ▪ political climate risk; ▪ physical climate risk; ▪ cultural or language; ▪ time-zones; and ▪ employment conditions in offshore jurisdictions. Firms must also ensure: ▪ that contracts for outsourced arrangements, including those which are offshored, provide that Firms and the Central Bank must be given access to carry out quality assurance and supervisory work; ▪ there are minimum standards in place at the OSP in respect of risk appetite; ▪ issues identified as part of the country risk assessment are also considered as part of the Firms DR / BCP and substitutability planning; and ▪ jurisdictional and other complications, which might arise in the event of insolvency, are considered closer.	☐

11 BITS Guide to Concentration Risk in Outsourcing Relationships.

7.	**Potential Constraints on Offshoring**	Firms may, if appropriate, be restricted from offshoring activities, where supervisibility is either severely constrained or non-existent. Firms should 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 and assess the criticality or importance of the proposed outsourcing arrangements at an early stage.	☐
8.	**Sensitive Data Risk**	In order to effectively manage risks relating to the potential loss, alteration, destruction or unauthorised disclosure of their sensitive data, Firms should: ▪ implement appropriate measures to secure their data and set out these measures in the Firms outsourcing policy and applicable contracts / written agreements; ▪ implement a documented data management strategy that addresses risks, including those relating to data transmission and storage including when offshored. The data management strategy must: ▪ define an approach to data security and management; ▪ address, in terms of location, data at rest, data in use and data in transit / transmission; ▪ consider and document data issues that might arise in the event of termination, insolvency and or recovery / resolution events; ▪ set out the standards and requirements to be applied in respect of the Firm's data including back-up and recovery, security protocols and encryption standards, access management and legal requirements; ▪ ensure that, where data is encrypted, Firms make provisions to guarantee that security measures are kept secure and accessible to the Central Bank; ▪ 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. ▪ consider guidelines / best practice frameworks in the context of information and data security; ▪ ensure adherence with the requirements of applicable data protection laws; and ▪ consider the principles of confidentiality, integrity, availability and authentication of data when conducting risk assessments.	☐

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).

4 Due Diligence Checklist

No	Due Diligence considerations when selecting an OSP	✓
	Firms must consider the following criteria when conducting the initial due diligence review in respect of OSPs:	
1.	What is the business model, nature, scale, complexity, financial situation, ownership and group structure of the OSP?	☐
2.	Are there long-term relationships with OSPs that have already been assessed and perform services for the Firm?	☐
3.	Is the OSP a parent undertaking or subsidiary of the Firm, is it part of the accounting scope of consolidation of the Firm, is it a member, or is it owned by firms that are members of the same group. For intragroup arrangements, consideration should be given to the extent of control or influence which may be exercised by the Firm.	☐
4.	Does the OSP comply with all applicable legal and regulatory requirements on data protection?	☐
5.	Is the OSP authorised by a regulatory authority to provide the service in question and is the OSP supervised by competent authorities?	☐
6.	Has the OSP capacity to keep pace with innovation within the market sector?	☐
7.	What is the OSP's business reputation including compliance, complaints and outstanding or potential litigation?	☐
8.	What is the financial performance of the OSP?	☐
9.	Are there any conflicts of interest, particularly in the case of intragroup arrangements?	☐
10.	What is the effectiveness of the OSP's risk management and internal controls, including IT and cybersecurity in providing appropriate technical and organisational measures to protect the data in accordance with the Firms data management strategy?	☐
11.	What is the substitutability of the OSP / CSP (identifying possible alternative or back-up providers)?	☐
12.	Is there a potential exposure to concentration risk?	☐
13.	Has the OSP an ability to demonstrate certified adherence to recognised, relevant industry standards?	☐
14.	Is the OSP open to negotiating mutually acceptable contractual and SLA provisions?	☐
15.	Are the proposed arrangements compatible with future development strategies of the Firm?	☐
16	Does the Firm have the necessary managerial skills to oversee the OSP and the skills within the OSP?	☐

17.	Has the employment and management of sub-contractors by the OSP been considered?	☐
18.	Has the reliance by the prospective OSP on and control over sub-contractors been considered?	☐
19.	Are the incident reporting and management programmes in the OSP adequate?	☐
20.	Does the OSP have insurance coverage?	☐
21.	Does the OSP have adequate resilience measures?	☐
22.	Is there cross-border activities that need to be considered?	☐
23.	Has the track record of the OSP in respect of termination arrangements without having an impact on the continuity or quality of operations been considered?	☐
24.	What is the 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?	☐
25.	Does the risk appetite of the OSP align with that of the Firm in order to avoid risk appetite breaches as a result of an OSP activity or failure?	☐
26.	Are the design and effectiveness of risk management controls at the OSP at least as strong as the controls utilised by the Firm itself?	☐

5 Central Bank Notification Obligations

No	Requirement	Guidance	✓
		Firms should consider the following reporting obligations in respect of critical or important outsourcing arrangements	
1.	**Provision of Outsourcing Information to the Central Bank**	The Central Bank expects to be notified of proposed "critical or important" outsourcing arrangements.	☐
2.	**Notification - General**	Firms are required to assess the criticality or importance of proposed outsourcing arrangements at an early stage. In this context, Firms may be requested to: ▪ provide information on the output from the due diligence and/or risk assessments conducted; ▪ enhance its due diligence review, upgrade its governance and/or risk management arrangements and delay entering into an agreement until such are satisfactory; and ▪ amend proposed contracts, written agreements or SLAs to ensure regulatory compliance and ensure delivery on regulatory expectations in respect of risk management.	☐
3.	**Notification - Offshore Jurisdictions**	Firms are required 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.	☐

4	**Notification – content**	The notification of a proposed new critical or important outsourcing arrangement should contain the following information: ▪ a reference number for the proposed critical or important outsourcing arrangement; ▪ 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 Firm if known; ▪ 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; ▪ a category assigned by the Firm that reflects the nature of the function (eg, IT, control function), which should facilitate the identification of different types of arrangements; ▪ 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; ▪ the country or countries where the service is to be performed, including the location of the storage and or processing of data; ▪ brief summary of why the outsourced function is considered critical or important; ▪ the date of the assessment of the criticality or importance of the outsourced function. ▪ in the case of outsourcing to a CSP, the cloud service and deployment models, and the specific nature of the data to be held and the locations where such data will be stored and or processed; ▪ the Firms within the scope of the prudential consolidation, that will make use of the outsourcing arrangement; ▪ whether or not the OSP or sub-service provider is part of the group or is owned by the Firm or other members within the group; ▪ the date of the most recent risk assessment conducted in respect of the proposed arrangement and a brief summary of the main results; ▪ the individual or decision-making body in the Firm that approved the proposed outsourcing arrangement; ▪ the governing law of the proposed outsourcing agreement; ▪ 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; ▪ where the data will be stored and or processed; ▪ the outcome of the assessment of the service provider's substitutability; ▪ whether the proposed outsourced critical or important function supports business operations that are time-critical; and ▪ the estimated annual budget cost of the outsourcing arrangement.

5.	**Supervisory Response to Notifications**	Firms should note that 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.	☐
6.	**Reporting of Adverse Incidents**	Firms are required to report to the Central Bank when the following occur in respect of outsourcing arrangements: ▪ matters / events giving rise to a significant change to the outsourcing aspects of the business model; ▪ a material event, which affects the provision of critical or important services by an OSP; and ▪ material breaches of contractual arrangements or SLAs which affects the provision of regulated services by the Firm or adversely affects customers / consumers.	☐
7.	**Additional Information**	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. The Central Bank may require Firms to provide detailed information on any outsourcing arrangement, even if the function concerned is not considered critical or important.	☐

No	Requirement	Guidance	✓
		The key requirements for documenting an outsourcing arrangement in respect of critical or important functions are set out below:	
1.	**Contractual Arrangements and SLAa**	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 SLAs.	☐
2.	**Contractual Arrangements and Intragroup arrangements**	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 Firm and the contract should provide for same.	☐
3.	**Terms of Outsourcing Agreement – General**	Contracts or written agreements governing the provision of critical or important functions or services, should be resolution resilient and in line with the EBA Guidelines on Outsourcing[13]. Firms must ensure the following provisions are included: ▪ a clear description of the outsourced function or services to be provided; ▪ the start date and end date (or renewal date) of the contract / agreement and the notice periods for the OSP and the Firm; ▪ the governing law of the agreement; ▪ the parties' financial obligations; ▪ the location(s) 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 Firm, in advance, if the OSP / CSP proposes to change location; ▪ whether the OSP should take out mandatory insurance against certain risks and, if applicable, the level of insurance cover requested; ▪ the requirements to implement and test BCP; ▪ termination rights and exit strategies covering both stressed and non-stressed scenarios. Both parties should commit to take reasonable steps to support the testing of a Firm's exit strategies / termination plans; ▪ the obligation of the OSP / CSP to cooperate with the Central Bank and the resolution authority of the Firm including other persons appointed by them; ▪ to ensure resolution resiliency where applicable; ▪ the unrestricted right of Firms and the Central Bank to inspect and audit the OSP / CSP; and ▪ that where a situation of recovery and or resolution arises it cannot be deemed to be grounds for termination of the outsourcing arrangement.	☐

13 EBA Guidelines on Outsourcing Arrangements EBA GL/2019/02

4.	**Terms of Outsourcing Agreement – Good practices**	As a matter of good practice, Firms should also include the following in contracts or written agreements in respect of critical or important services: ▪ dispute resolution arrangements containing provisions for remedies including penalty clauses for significant breaches of key performance indicators ("**KPIs**"); ▪ indemnification; ▪ limits and liability; ▪ provisions for amendment of contracts or written agreements; and ▪ notifications of financial difficulty, catastrophic events and significant incidents.	☐
5.	**Terms of Outsourcing Agreement – Sub-outsourcing**	The written agreement should specify whether the sub-outsourcing of a critical or important function is permitted and the conditions for sub-outsourcing. In this regard, the agreement should require OSPs to: ▪ notify Firms ahead of planned material changes to sub-outsourcing arrangements in a timely manner; ▪ obtain prior specific or general written authorisation where appropriate; ▪ give Firms the right to approve or object to material sub-outsourcing arrangements and / or terminate the agreement in certain circumstances; ▪ ensure that the Firms and the Central Bank's rights of access and audit apply in the case of any sub-outsourcing arrangement; and ▪ specify any functions or activities that are prohibited from being sub-outsourced.	☐
6.	**Terms of Outsourcing Agreement – Data Management / Security**	In respect of data management and security, the written agreement should specify: ▪ where control / custody of data is being outsourced; ▪ requirements regarding the accessibility, availability, integrity, confidentiality, privacy and safety of relevant data; ▪ that the controls should provide for appropriate and proportionate information security related objectives; ▪ that the reporting obligations of the OSP to the Firm should require timely reporting against the KPIs, which provides actionable MI to the Firm; ▪ provisions that ensure that the data owned by the Firm can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the OSP / CSP. 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.	☐
7.	**Terms of Outsourcing Agreement – Performance Monitoring**	The written agreement governing the provision of critical or important functions or services should specify: ▪ the right of the Firm to monitor the OSP's performance on an ongoing basis by reference to KPIs; and ▪ the agreed service levels, which should include precise quantitative and qualitative performance targets (using KPIs to track) for the outsourced function.	☐

8.	**Termination Rights**	The contract or written agreement should expressly allow the possibility for the Firm to terminate the arrangement, in accordance with applicable law, including, in the following situations: ▪ where the OSP is in breach of applicable law, regulations or contractual provisions; ▪ where impediments capable of altering the performance of the outsourced function are identified; ▪ where there are material changes affecting the outsourcing arrangement or the OSP; ▪ where there are weaknesses in the data management framework; and ▪ where instructions to terminate are given by the Central Bank.	☐
9.	**Termination Rights – Transfer Obligations**	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 Firm. The contract or written agreement should: ▪ 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 Firm, including the treatment of data; ▪ set an appropriate transition period, during which the OSP, after the termination of the outsourcing arrangement, would continue to provide the outsourced; and ▪ include an obligation on the OSP to support the Firm in the orderly transfer.	☐
10.	**Access, Information and Audit Rights**	Firms should ensure that within the contract or written outsourcing agreement, the OSP grants the Firm and their competent authorities, including resolution authorities, and any other person appointed by them or the competent authorities, full access to all relevant business premises and unrestricted rights of inspection and audit related to the outsourcing arrangement. Firms must exercise their access and audit rights, determine the audit frequency and areas to be audited using a risk-based approach and adhere to relevant, commonly accepted, national and international audit standards.	☐
11.	**Non-Critical or Important Outsourcing Arrangements**	Written agreements for non-critical or less important outsourcing arrangements should include appropriate contractual safeguards to manage relevant risks.	☐
12.	**Values and Ethical Behaviour – Regulatory Expectations**	In line with the EBA Guidelines on Outsourcing[14] and general good practices, Firms should take appropriate steps to ensure that OSPs act in a manner consistent with the values and code of conduct of the Firm. Firms should also satisfy themselves that OSPs located in third countries and if applicable, their sub-contractors, act in an ethical and socially responsible manner and adhere to international standards on human rights, environmental protection and appropriate working conditions, including the prohibition of child labour.	☐

14 EBA Guidelines on Outsourcing Arrangements EBA GL/2019/02.

7 The Outsourcing Register

The below requirements have been prepared in line with the requirements as set out in the Outsourcing Guidance as published by the Central Bank in December 2021, any deviations from these requirements in the Central Bank's sectoral submission templates published in August 2022 will be highlighted below.

No	Requirement	Guidance	✓
The Guidance has outlined a new requirement which requires Firms to establish and maintain an outsourcing register (the "**Register**"), which should contain the following information:			
1.	**The Register - OSPs**	Firms must establish and maintain an outsourcing register. The register should include at least the following information, for all existing and future outsourcing arrangements: ▪ a reference number for each outsourcing arrangement; ▪ 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 Firm; ▪ a brief description of the outsourced function, including the data that are outsourced and whether personal data has been transferred or if the processing of personal data is outsourced to a service provider; ▪ a category assigned by the Firm that reflects the nature of the function; ▪ 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; ▪ the country or countries where the service is to be performed, including the location of the data; ▪ whether or not 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; ▪ in the case of outsourcing to a CSP, the cloud service and deployment models and the specific nature of the data to be held and the locations where such data will be stored; and ▪ the date of the most recent assessment of the criticality or importance of the outsourced function.	☐
2.	**Contractual Arrangements and Intragroup arrangements**	In addition, the register should include at least the following information, for all existing and future outsourcing arrangements so that it is maintained up-to-date: ▪ total number of outsourced service arrangements in place; ▪ total number of critical or important outsourced arrangements in place; ▪ total number of arrangements with CSPs; ▪ confirmation that a Firm has an outsourcing risk management framework in place; ▪ confirmation that a Firm has an outsourcing policy in place; ▪ confirmation that the outsourcing policy is approved by the board or equivalent; ▪ details of provision by the Firm of outsourcing service(s) to other Firms; and ▪ confirmation that contracts / written Agreements are supported by SLAs.	☐

3.	**The Register - Additional Requirements for Critical / Important Functions**	The Firm must ensure that the Register also includes the following additional information for critical / important fuctions: ▪ 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; ▪ whether or not the service provider or sub-service provider is part of the group or is owned by firms within the group; ▪ the date 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; ▪ the individual or decision-making body in the Firm that approved the outsourcing arrangement; ▪ the governing law of the outsourcing agreement; ▪ the dates of the most recent and next scheduled audits and reviews, where applicable; ▪ 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 subcontractors are registered, where the service will be performed and, if applicable, the location where the data will be stored; ▪ an outcome of the assessment of the service provider's substitutability, 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; ▪ identification of alternative service providers; ▪ whether the outsourced critical or important function supports business operations that are time-critical; ▪ confirmation and latest dates of the testing of the firms BCP's and exit strategies; ▪ confirmation and dates of testing of OSP's BCP; ▪ the estimated annual budget cost; and ▪ a record of terminated arrangements for an appropriate retention period.	☐
4.	**Submission of the Register**	The Central Bank has noted that the submission of the data contained in a Firm's register will be by way of a periodic regulatory return. The frequency and timing of such returns will be specified to sectors by way of a supervisory communication[16].	☐

16 Section 10.2.1, Cross-Industry Guidance on Outsourcing December 2021.

Central Bank Sectoral Guidance on the Submission of Outsourcing Registers

On 10 August 2022, the Central Bank published sectoral guidance notes and templates for the submission of firm's registers for the following sectors (Re)Insurance Undertakings, Less Significant Institutions ("**LSIs**"), Markets Firms or Regulated Financial Service Providers and Payments & E-Money Institutions.

All firms whose PRISM Impact Rating is Medium Low or above are required to submit their outsourcing register to the Central Bank via the Online Reporting System ("**ONR**") using the relevant sectoral reporting template on an annual basis.

Low Impact firms may also be asked to submit their outsourcing register on a case by case basis by their supervisor. Relevant firms should use the relevant industry template to guide the completion of their registers and be prepared to provide the register to supervisors on request or as part of a subsequent collection of registers by the Central Bank. The first reference date for the submission of data for the outsourcing arrangements is 31 December 2021. In scope firms should submit their register with data complete as of 31 December 2021 and only include contracts / written agreements with a start date before that date. Firms are requested to submit their first completed register via the ONR by close of business on 07 October 2022.

The submission deadline from 2023 onwards will be end-February of each year, with the reference date of 31 December of the previous year. The submission deadline for 2023 will be confirmed by the Central Bank in due course.

Notable changes

The submission templates published by the Central Bank for the submission by Firms of their Outsourcing Register mostly align with the requirements as published in the Outsourcing Guidance, however, there a some notable changes which are highlighted below:

- Under the additional requirements for critical/important functions, the Central Bank sectoral submission templates require firms to confirm if the terms of the contract have been reviewed and are in compliance with the Cross Industry Guidance on Outsourcing and relevant national laws. This confirmation is not required under the Outsourcing Guidance;
- Under the additional requirements for critical/important functions, the Outsourcing Guidance notes that the register should include whether or not the service provider or sub-service provider is part of the group or is owned by firms within the group. The Central Bank sectoral submission templates do not request this confirmation;
- Under the additional requirements for critical/important functions, the Outsourcing Guidance notes that the register should include confirmation and latest dates of the testing of the firm's BCPs and exit strategies and the OSPs BNPs. The Central Bank sectoral submission templates also request that this information be provided in respect of all outsourcing arrangements and additionally that detail or commentary be provided on these tests;
- Under the additional requirements for critical/important functions, the Outsourcing Guidance notes that the register should include a record of terminated arrangements for an appropriate retention period. The Central Bank sectoral submission templates does not request detail of these but instead requests confirmation that of a record terminated agreements exists for all terminated outsourcing arrangements for an appropriate period;
- Under the additional requirements for critical/important functions, the Outsourcing Guidance notes that 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 subcontractors are registered, where the service will be performed and, if applicable, the location where the data will be stored. In addition to the above, the Central Bank's sectoral submission templates also request confirmation of whether there is a possibility of sub outsourcing and if there will be any transfer or processing of personal data to/by contractor for sub-outsourcing of material parts; and
- Under the additional requirements for critical/important functions, the Outsourcing Guidance notes that the register should include a record of terminated arrangements for an appropriate retention period.

8 Monitoring and Oversight of the Outsourcing arrangement

No	Requirement	Guidance	✓
		Firms should consider the following requirements to ensure that effective oversight of outsourced of the arrangement is maintained:	
1.	**Ongoing Monitoring and Challenge**	Firms should incorporate outsourcing assurance into its three lines of defence.	☐

2.	**Monitoring of outsourcing arrangements**	Firms must implement appropriate mechanisms to oversee the performance of their outsourced arrangements. Firms should ensure the following measures are considered:
		▪ have sufficient and appropriately skilled staff;
		▪ identify key decision makers who have the ability and capability to make decisions;
		▪ monitor the performance of the OSP using a risk based approach, including by:
		  ▪ ensuring receipt of appropriate reports from the OSP;
		  ▪ assessing the performance of the OSP;
		  ▪ assessing the adequacy of the OSP's BCM and associated testing and the effectiveness of the integration; and
		  ▪ conducting onsite reviews of the OSP.
		▪ take appropriate measures to ensure that any deficiencies identified in the provision of the service by the OSP are effectively addressed and remediated; and
		▪ incorporate assurance testing related to the management and monitoring of outsourcing as part of its risk management and compliance monitoring programmes.
			☐

3.	**Risk Assessment & Monitoring**	A Firm must regularly review its outsourcing arrangements, with particular focus on its critical or important arrangements. Such reviews should consider whether: ▪ the nature, scale or complexity of the outsourced function or the risks associated with it have changed since its inception or last review; ▪ 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 ▪ there have been any changes in the Firm's exposure to concentration risk. A firm must review and refresh their risk assessments on a periodic basis to ensure that it continues to accurately reflect the Firm's business.	☐
4.	**Review of Agreements**	Written agreements and contracts should be reviewed periodically. Reviews should also be scheduled in sufficient time in advance of renewals or termination dates to ensure smooth transitions or continuity of service.	☐

5.	**Internal Audit & Independent Third Party Review**	Firms should 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, using a risk based approach, the audit programme of the internal audit function assesses: ▪ if the Firm's outsourcing framework is operating effectively and in line with the outsourcing policy and the Firm's risk appetite; ▪ whether the outsourcing policy and associated control framework have been reviewed and updated appropriately; ▪ that outsourcing arrangements are being correctly classified in line with the Firm's methodology for the assessment of "criticality and importance"; ▪ that the Firm's register is being appropriately maintained to ensure accuracy and currency; ▪ the adequacy and appropriateness of the Firm's outsourcing risk assessment generally; ▪ effectiveness of the oversight and direction of the board, senior management or management body and any relevant committees in respect of outsourcing; ▪ effectiveness of the Firm's monitoring and management of its outsourcing arrangements; and ▪ operation by the OSP of the underlying outsourced activities or functions via onsite audits. Firms must ensure that the party conducting the audit has the necessary skills and expertise to conduct the review effectively and to comprehensively assess and report on the outcomes.	☐
6.	**Use of Third Party Certifications and Pooled Audits**	Where Firms utilise third party certifications provided by the OSP and / or pooled audits, Firms must 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. The Firm must also be able to evidence that: ▪ the scope and process for the review is appropriate, and provides sufficient coverage of the outsourced activities and functions and related risk management controls; ▪ the review criteria are up to date and take account of all relevant legal and regulatory requirements; ▪ the third party commissioned to conduct the review has the appropriate skills and expertise; and ▪ the Firm has the appropriate skills and expertise to review, challenge and make informed decisions as to the quality and outcomes of the review.	☐

7.	**Due Diligence**	Firms must ensure that appropriate and proportionate due diligence reviews are conducted with the following frequency: ▪ periodically over the lifecycle of the contract to review the financial health of key OSPs, providing critical or important services; ▪ annually for key OSPs of critical or important services and a brief review of the financial health should be conducted each year; and ▪ 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.	☐
8.	**Critical or Important Assessment**	The Firm should conduct a review, in respect of the assessment of criticality or importance at a minimum: ▪ prior to signing an outsourcing contract or written outsource agreement; ▪ at appropriate intervals thereafter; ▪ where a Firm plans to scale up its use of the service or dependency on the OSP; and / or ▪ if an organisational change at the OSP or a material sub-outsourced service provider occurs.	☐

No	Requirement	Guidance	✓
The general requirements that Firms must consider when implementing a data management framework when outsourcing criticality or important functions			
1.	**Comprehensive security architecture**	Firms must design a comprehensive security architecture. Standards for configuring cloud services should ensure consistency of application of security measures on own premises and in the cloud. Firms need to understand the different cloud deployment models and the service offerings available to them.	☐
2.	**Data Security - Availability and Integrity**	Firms must implement operationally effective controls for data-in-transit, data-in-memory and data-at-rest. These controls should include a mix of preventative and detective measures, including the following: ▪ configuration management; ▪ encryption and key management; ▪ identity and access management; ▪ access and activity logging; ▪ incident detection and response; ▪ loss prevention and recovery; ▪ data segregation (if using a multi-tenant environment – cloud or other); ▪ operating system, network and firewall configuration; ▪ staff training; ▪ the ongoing monitoring of the effectiveness of the OSP's controls; ▪ policies and procedures to detect activities that may impact firms' information security; ▪ procedures for the deletion of a Firm's data from all the locations where the OSP / CSP may have stored it following an exit / termination; and ▪ contractual rights to audit the OSP data storage and management systems.	☐

10 Exit Strategy

No	Requirement	Guidance	✓
		Firms should plan and implement an effective exit strategy in the event of an expected / unexpected termination of an outsourcing contract, as set out below.	
1.	**Exit Strategies – General**	In respect of exit strategies, Firms should ensure that: ▪ it has considered and documented the impact tolerances for business service interruptions; ▪ it has a clearly defined and documented exit strategy in place, which is viable, appropriately planned, documented and regularly tested; ▪ it assesses whether an OSP can be substituted; ▪ the exit strategy includes arrangements for reintegration of services within the Firm or group entity, either where an alternative provider is not available or in cases where reintegration is required by regulation; ▪ it considers, plan and test scenarios which may warrant the transfer of activities; ▪ it develops and maintain skills and expertise so that functions can, if required, be taken back in-house by the Firm or transferred to an alternative provider; ▪ 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; ▪ its considers and implement within its exit strategy, contingency arrangements to cover the interim period between invoking an exit strategy and the ultimate transfer; ▪ there is appropriate understanding and oversight of the data flows between the Firm and the OSP; ▪ it has considered the potential for and implications of "step-in risk" materialising in the context of stressed scenarios. Firms should determine the viability of invoking 'step-in' rights in such scenarios; and ▪ such plans are viable and can be executed accordingly.	☐
2.	**Exit Strategies Intra-Group Arrangements**	Firms must ensure that, in the case of intragroup arrangements, where Firms avail of exit plans that have been established at a group level, the plans address the Central Bank's expectations and relevant sectoral legislation and regulatory requirements.	☐
3.	**Exit Strategies – Cloud Outsourcing Arrangements**	In the specific case of critical or important cloud outsourcing arrangements, Firms should 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.	
4.	**Exit Strategies – Review**	Firms must 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.	

Matheson

DUBLIN
70 Sir John Rogerson's Quay,
Dublin 2
Ireland

T: +353 1 232 2000
E: dublin@matheson.com

CORK
Penrose One,
Renrose Dock,
Cork, T23KW81

T: +353 21 465 8200
E: cork@matheson.com

LONDON
1 Love Lane
London EC2N 7JN
England

T: +44 20 7614 5670
E: london@matheson.com

NEW YORK
200 Park Avenue
New York, NY 10166
United States

T: +1 646 354 6582
E: newyork@matheson.com

PALO ALTO
530 Lytton Avenue
Palo Alto, CA 94301
United States

T: +1 650 617 3351
E: paloalto@matheson.com

SAN FRANCISCO
156 2nd Street
San Francisco CA 94105
United States

T: +1 650 617 3351
E: sf@matheson.com