



Banc Ceannais na hÉireann
Central Bank of Ireland

Eurosystem

Draft Guidance on Good Practices for the Sound Management of Third-Party Risks

October 2026

Contents

Introduction	3
1 Background	3
2 Context	5
3 The Reason for this Guidance.....	6
4 Layout of this Guidance	7
5 How this Guidance is to be Used	9
6 Critical or Important Functions and Services.....	10
7 Terminology	12
8 Effective date	12
Guidance on Good Practices for the Sound Management of Third-Party Risks.....	13
A. Governance and Organisational Context.....	13
B. Due Diligence and Risk Assessment.....	18
C. Contracting.....	22
D. Ongoing Risk Management and Monitoring.....	25
E. Incident and Termination Management	35

Introduction

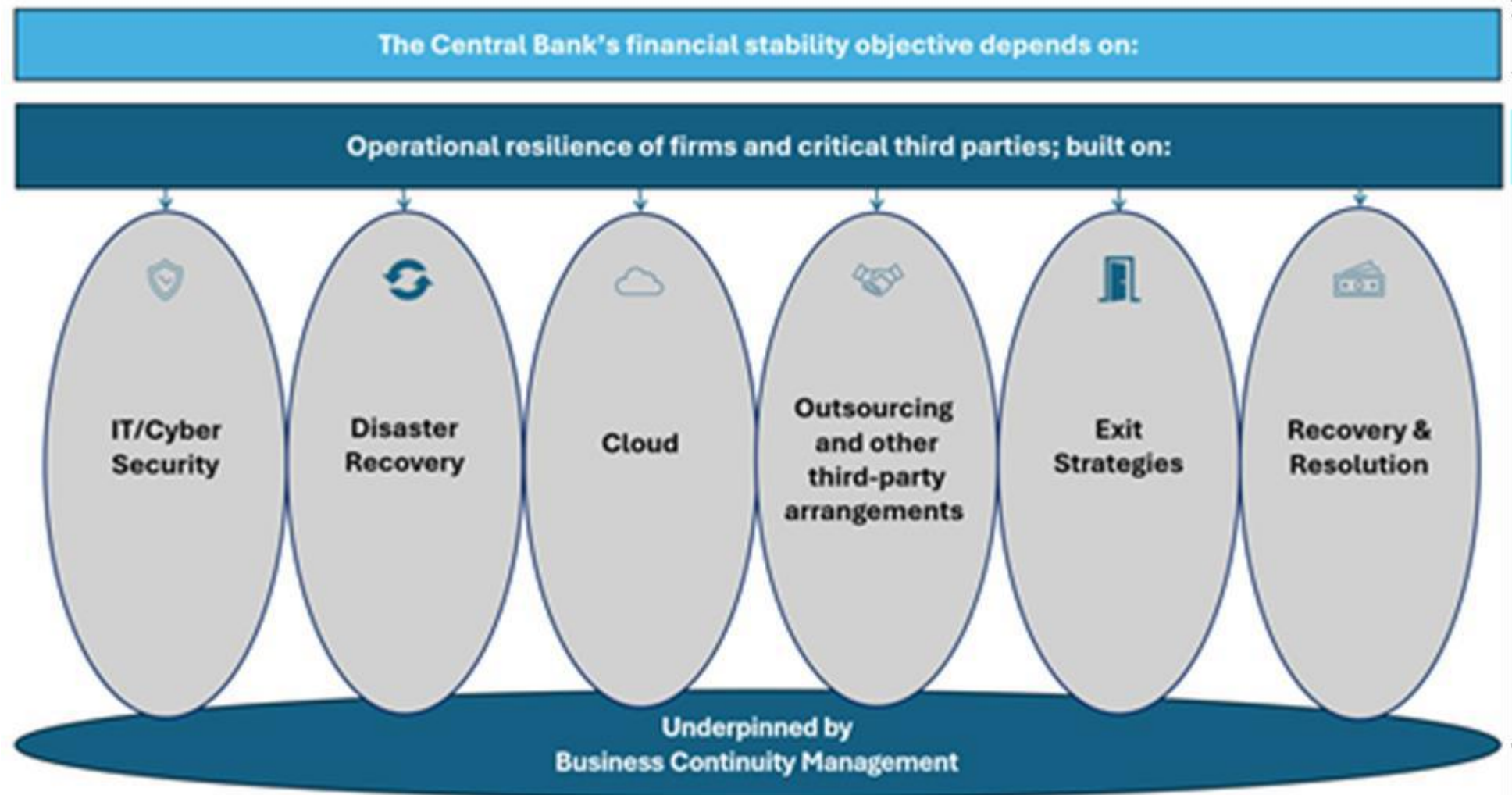
1 Background

- 1.1 The mission of the Central Bank of Ireland (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.
- 1.2 This Guidance contributes to:
- the resilience and stability of the financial system; and
 - the proper and effective regulation of financial service providers and markets, while ensuring that the best interests of consumers of financial services are protected.
- 1.3 The Central Bank remains strongly focused on outsourcing and all forms of third-party risk¹ management 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 and the Irish financial system.
- 1.4 The Central Bank's Operational Resilience Guidance² provides firms with an overarching holistic high-level view of the Central Bank's expectations in respect of the management of the building blocks of operational resilience, including outsourcing and third-party risk management. To ensure the required level of resilience throughout the system it is essential that firms appropriately address each of the foundational building blocks of resilience in a holistic fashion rather than in separate silos. The diagram below describes these building blocks, which are interrelated, interdependent, and underpinned by effective Business Continuity Management.
- 1.5 Sound management of third-party risks contributes directly to the safety and soundness of regulated financial service providers and the services they provide to the wider economy. From a systemic perspective, risks can be amplified through dependencies on a small number of third-party service providers, with the potential for rapid contagion when incidents occur.

¹“Third-party risks” in this Guidance intends to refer to any arrangement between a firm and a third-party service provider, including intragroup arrangements, for the provision of services or support to the firm on an ongoing or recurring basis. This includes, but is not limited to, traditional outsourcing arrangements.

² <https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp140/cross-industry-guidance-on-operational-resilience.pdf>

Figure 1 – Building Blocks of Operational Resilience



2 Context

- 2.1 The financial services landscape is continually evolving, influenced by customer preferences, technological innovation, regulatory developments, and changes in business models driven by cost, data capabilities, profitability and the need for increased flexibility. Outsourcing and the use of third parties continues to be a key strategic tool enabling regulated firms to respond to these changes, providing significant benefits but also posing risks to resilience if not effectively managed.
- 2.2 The Central Bank recognises the increasing reliance of many regulated firms on third-party service providers, including ICT service providers, as a driver of risk to both individual firms and, in some cases, to the system as a whole. This includes the use of both intragroup entities and external third parties, both regulated and unregulated, for activities and services considered central to the successful delivery of regulated firms' strategic objectives. Intragroup arrangements should be approached in the same manner as those arrangements with external third-party service providers, although the assessment and management of the risks presented by intragroup arrangements will be different.
- 2.3 Concerns relating to the continuity of service provision can also arise from intra-entity arrangements, and while such relationships are not specifically addressed by this Guidance, the risk needs to be appropriately managed. Firms should consider having formal arrangements in place for branches, to enable branches to comply with their obligations and commitments. Good practices in this Guidance may also be relevant for how branches manage the risks to service continuity.
- 2.4 New structures and business models are emerging to deliver critical or important services to financial services entities, with many capabilities increasingly controlled by service providers outside the traditional boundaries of the regulated financial services industry. This is leading to new service delivery models such as strategic partnering, cross-industry shared service centres, staff sharing and extensive sub-outsourcing.
- 2.5 Oversight of outsourcing can be complicated by sub-outsourcing (also referred to as chain outsourcing or sub-contracting), whereby the service provider transfers performance of an outsourced function to another provider. Outsourcing chains can become long and complex. Firms should ensure that sub-outsourcing does not impair a firm's visibility of activities being performed.
- 2.6 The increasing use of outsourcing and reliance on third parties also gives rise to growing concentration risk concerns, both at individual firm level and at sectoral

or system-wide level. Concentration risk is of particular concern where there are a limited number of providers of certain services, for example cloud service providers or other specialist service providers, that may be difficult to substitute. Such concentrations can give rise to broader systemic concentration risk concerns if not appropriately managed.

3 The Reason for this Guidance

- 3.1 Many financial services firms are subject to legal obligations with respect to the management of their risks, including risks presented through reliance on third parties. This is important to the stability and viability of regulated firms, the continued proper provision of services to consumers, and the efficient operation of the financial system more broadly.
- 3.2 Those firms subject to legal obligations to soundly and effectively manage third-party risks are not always provided with sufficient detail in the laws, regulations and guidelines to understand precisely what good management of these risks looks like. For those cases, the Central Bank is therefore providing guidance on appropriate good practices that should be considered by firms when reliant on third parties for the provision of services, especially those services that are critical or important to the proper functioning of the firm.
- 3.3 In some cases, the applicable legal framework contains detailed prescriptive requirements for the management of third-party risks. For example:
 - Firms subject to the EU Digital Operational Risk Act (DORA) are subject to detailed regulatory requirements for ICT third-party service providers (to the extent covered by DORA).
 - Firms subject to the binding Guidelines on the sound management of third-party risk regarding non-ICT services issued by the European Banking Authority³ have detailed regulatory requirements for third-party risks not subject to DORA⁴.

³<https://www.eba.europa.eu/sites/default/files/2026-09/dc9ccbb3-79b9-493d-b693-c21adeffbcc9/Final%20report%20on%20GL%20on%20third-party%20risk%20management.pdf>

⁴The EBA Guidelines apply to financial institutions as defined in Article 4(1) of Regulation No 1093/2010 that are institutions as defined in point (3) of Article 4(1) of Regulation (EU) No 575/2013 (CRR), third-country branches, as defined in point 1 of Article 47(3) of Directive 2013/36/EU, investment firms as defined in point (1) of Article 4(1) of Directive (EU) 2014/65 (MiFID II) with the exception of small and non-interconnected investment firms under Article 12(1) of Regulation (EU) 2019/2033, payment institutions as defined in Article 4(4) of Directive (EU) 2015/2336, electronic money institutions within the meaning of Directive 2009/110/EC and, issuers of asset referenced tokens (ARTs) as defined in Article 3(1), point 10 of Regulation (EU) 2023/1114.

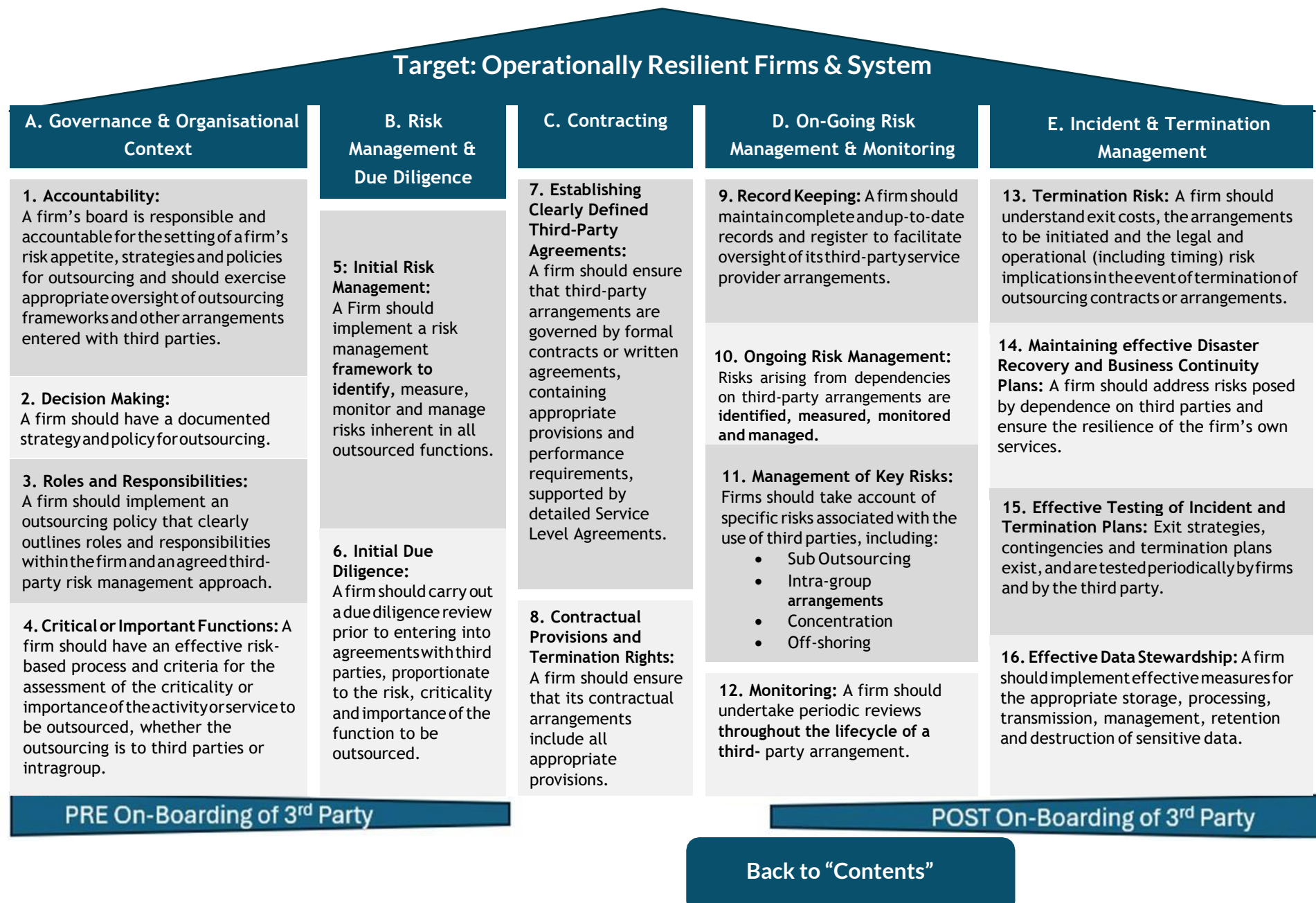
- 3.4 So, for example, credit institutions or payment institutions authorised in Ireland and complying with DORA for their ICT third-party risks, and with the EBA Guidelines for third-party risk management not covered by DORA, may find that this Guidance provides only limited additional insight⁵.
- 3.5 The regulatory provisions applicable to other firms (for example, insurance undertakings or retail credit firms, among others) may contain high-level obligations to manage risks, without sufficient descriptive provisions showing how those obligations can be complied with in practice. This Guidance seeks to bridge that gap.

4 Layout of this Guidance

- 4.1 The Guidance has been sequenced to appropriately reflect the identification of, and engagement by, firms with third parties and the subsequent management of those relationships. The Guidance is presented in discrete blocks of outcomes to be achieved, and practices that allow firms to benchmark the maturity of their own risk management practices. Figure 2 (below) shows the layout of the approach adopted in this Guidance.

⁵ In some cases, the EBA Guidelines do not apply to some third-party relationships: for example, “a financial service that is legally required to be performed by another regulated financial entity”. Where the EBA Guidelines do not apply, strict adherence to the EBA Guidelines is not required. This does not mean, however, that there is no third-party risk that needs to be managed. In such cases, firms are still expected to soundly and effectively manage the risks that a third-party relationship presents to firms, and to take such steps to manage those risks as might be reasonably required in the circumstances based on the nature of the relationship and the nature of the services provided.

Figure 2 – Sequencing of the Guidance



- 4.2 A firm should give consideration to the good practices identified in this document. Some are identified as foundational and others support the implementation of these foundations. It is intended that the good practices should be applied in respect of a firm's critical or important third-party arrangements, except where highlighted that the practices should take account of all third-party arrangements. However, firms should determine where it might be prudent to apply the practices to non-critical or less important arrangements in line with their own risk assessment.

5 How this Guidance is to be Used

- 5.1 In line with our supervisory approach, the Central Bank expects that Boards, senior management, and relevant staff within regulated firms should duly consider the appropriate application of this Guidance within their firm's operations. This document is also intended to assist anyone involved in the oversight, management, risk management, or provision of, third-party services for regulated firms in Ireland.
- 5.2 Where financial services firms are under a legal or regulatory obligation to manage their third-party risks to a particular standard, it is the responsibility of the firm to meet this standard. With this responsibility comes the ownership of decisions and the discretion to take and implement those decisions. Unless there are detailed prescriptive frameworks in place (such as DORA or the EBA Guidelines), the regulatory framework does not dictate to firms what governance arrangements, management structures or tools should be adopted, or what decisions should be made on entering or managing third-party arrangements.
- 5.3 Responsibility for risk identification, management and mitigation rests first and foremost with the board and management teams of firms. The Central Bank will use its knowledge, expertise and experience to assess whether the arrangements put in place by firms to govern and manage third-party risks are sufficiently sound and effective, and whether appropriate risk management outcomes have been achieved.
- 5.4 This Guidance will inform Central Bank staff in the same way as it informs firms. This does not mean that firms must adhere rigidly in all circumstances to these good practices (unless required to do so within their sectoral rules). The Central Bank recognises that firms are best placed to identify the risks to which they are exposed, to assess the importance of those risks, and how best to manage them, including assessing whether they fall within a firm's risk appetite. However, the Central Bank may require firms to demonstrate appropriate consideration of the topics covered within this document in reaching those decisions.

- 5.5 As explained in Our Approach to Supervision⁶, the Central Bank takes a risk-based approach to supervision. The Central Bank's assessment will be based on the principle of proportionality i.e. the nature, scale and complexity of the business will dictate the degree of risk that will need to be managed and the impact that failure to do so properly will have. In circumstances where the risks to the firm, the financial system, or to consumers of financial services are sufficiently high, the Central Bank will intervene to require a strengthening of the firm's existing or proposed risk management practices.
- 5.6 To ensure that the Central Bank can fulfil its role in ensuring that the financial system operates in the best interests of consumers and the wider economy, the Central Bank periodically collects information on the use of third-party services by regulated firms. This data provides key information on the build-up of systemic concentration risks and ensures that the Central Bank can identify as early as possible where incidents involving third-party service providers may have a systemic impact. The information that the Central Bank requests from firms must be complete, consistent and in a form that permits the Central Bank to efficiently process and analyse. The information register that the Central Bank collects from firms is information which firms are reasonably expected to record and track as part of their own management of third-party risks. Firms should ensure, therefore, that their records are maintained in the form that the Central Bank requests, and are kept up to date. The templates for maintenance and submission of that information are set out on the Central Bank's website⁷.

6 Critical or Important Functions and Services

- 6.1 For the purpose of this Guidance, the good practices set out should be applied in respect of a firm's critical or important third-party arrangements. 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.
- 6.2 Where the provision by a firm of critical or important services, or the performance by a firm of critical or important functions depends on the full and proper fulfilment of obligations by third parties, a firm must take proportionately stronger measures to manage that risk.
- 6.3 Firms themselves determine what services provided to them by third parties underpin the proper performance by the firm of its services and functions. This will vary from firm to firm. The third-party service becomes critical or important where the failure to provide that service directly or indirectly would prevent the

⁶<https://www.centralbank.ie/docs/default-source/regulation/transforming-regulation-and-supervision/our-approach-to-supervision.pdf>

⁷<https://www.centralbank.ie/regulation/outsourcing-registers-submission-requirements>

firm from carrying out its core operations, fulfilling its functions, providing its services to its customers, or negatively impact the normal functioning of the financial system.

- 6.4 A firm may not initially identify a reliance on a third-party arrangement as being important or critical, but that status may change over time. Firms need to properly oversee and manage all of their third-party dependencies and monitor if the reliance by the firm on a third party increases in importance or criticality.
- 6.5 There is no science to the use of the terms ‘critical’ or ‘important’. The idea is to identify what is critical or important to the ability of a firm to function, or to provide services to its customers, including the financial stability of the firm and its ability to comply with laws and regulations. What is vital is that a firm understands the risks to which it is exposed by reliance on third parties and that the firm soundly, effectively and proportionately manages those risks for the benefit of the firm and the firm’s customers. It is the responsibility of an individual firm to identify the criteria it uses to define what is critical or important in the context of its business model.
- 6.6 While the management response to risks posed to critical or important functions, or by the risks posed by the provision of critical or important services, will clearly be more substantial, firms should nevertheless seek to identify, record and appropriately manage all third-party risks to which they are exposed as part of a robust overall risk management strategy.
- 6.7 While the emphasis in this Guidance is on the management of risk to firms present in third party arrangements, firms should also ensure that third-party arrangements must not create impediments to the resolvability of the financial entity where applicable. Where firms are subject to regulatory frameworks that seek to promote resolution and recovery of firms, those firms must also understand what ‘critical functions’ and ‘importance’ means precisely⁸ in the context of those other frameworks, and the obligations imposed under those frameworks.

Notifications

- 6.8 Within the legal and regulatory requirements that apply, some firms are obliged to notify the Central Bank when it is proposed to outsource critical or important functions or services, and where issues arise with such third-party arrangements. A firm should consult the Central Bank website when considering when and how to make a notification.

⁸ And separately and distinctly.

7 Terminology

- 7.1 This Guidance makes references interchangeably to ‘outsourcing’ and other third-party arrangements. While a significant proportion of exposure to third-party risk arises in the form of what is traditionally regarded as outsourcing, there are other arrangements that firms can enter into with third parties that create a reliance by a firm on that third-party e.g. partnerships and joint ventures. Outsourcing also includes arrangements for the provision of services by an intragroup service provider.
- 7.2 References in this document to ‘board’ include ‘governing or management body’ of a firm.
- 7.3 References to the Central Bank reflect that this document is generally directed at firms regulated by the Central Bank. However, when the document references competent or regulatory authorities generally, these can be any competent regulator that has authority over a firm, or over a third party for the business of that third party.
- 7.4 In certain legislation, regulations and guidance, there is use of the term ‘delegation’ to describe what is in effect the outsourcing of activities to third parties. “Delegation” and “outsourcing” are not considered by the Central Bank to be different concepts, as fundamentally the arrangements being entered into by a firm create a reliance on a third-party. Accordingly, when such reliance is created it would be good practice for a firm to ensure the proper oversight and management of the arrangements upon which the firm relies, however the arrangement might be described.
- 7.5 This Guidance is for the benefit of firms when seeking to understand how they might better manage the third-party risks to which they might be exposed. The Guidance uses the word “should” throughout to indicate opinion and advice on what is recommended as desirable for a firm to soundly and effectively manage third-party risks.

8 Effective date

- 8.1 Upon publication of this Guidance, this Guidance will replace the Cross-Industry Guidance on Outsourcing 2021 which will be considered withdrawn.

Guidance on Good Practices for the Sound Management of Third-Party Risks

A. Governance and Organisational Context

Outcome A1 – Accountability

A firm's board is responsible and accountable for the setting of a firm's strategies and policies (including the risk appetite and risk management framework) in relation to third-party arrangements and should have, and exercise appropriate oversight of outsourcing frameworks and other arrangements entered into with third parties.

Foundational good practices

- A1.1 Governing or management bodies should ensure that the appropriate structures are in place to facilitate a comprehensive view and oversight of their outsourcing and other third-party risk universe. Such oversight is a key element in assisting governing or management bodies to address their responsibilities with regard to the security and resilience of service provision. While the performance of functions and activities can be outsourced, governing or management bodies and senior management of regulated firms cannot outsource their responsibilities.
- A1.2 The governing or management body should ensure that there are appropriate and effective governance and internal controls to identify, measure, manage, monitor and report the risks associated with their outsourcing/third-party arrangements.
- A1.3 The governing or management body should ensure that appropriate skills and knowledge are maintained within the firm to effectively oversee outsourcing and other third-party arrangements, throughout the lifecycle, from inception to conclusion. This is especially important where the activities being outsourced are technical, e.g. ICT services, and/or complex in nature, for example in the case of outsourcing to cloud service providers.

Supporting good practices

- A1.4 The governing or management body should assign responsibility for oversight of third-party risk, and outsourcing and other third-party arrangements, to an appropriately designated individual, function and/or committee, to enable a

holistic view of third-party risk to be maintained and reported on. This designated function should be directly accountable to the governing or management body.

- A1.5 The governing or management body should ensure that there are appropriate structures and mechanisms in place to provide a comprehensive view of the firm's third-party universe to the governing or management body, including the provision of timely and appropriate management information which provides sufficient detail to enable the governing or management body to challenge the establishment and ongoing oversight of outsourcing and other third-party arrangements.

Outcome A2 – Decision Making

A firm should have in place a documented Strategy and Policy for outsourcing and other third-party arrangements.

Foundational good practices

- A2.1 As the appropriate decision-making authority within a firm, the governing or management body should ensure that there is a documented third-party risk strategy in place, which is aligned to the firm's business strategy, operating model, risk appetite, and risk management framework.
- A2.2 The third-party risk strategy should be supported through appropriate policies, procedures and controls.

Supporting good practices

- A2.3 In formulating a third-party risk strategy, consideration is given to areas including but not limited to:
- i. the extent of outsourcing, both independent and intragroup, that is proposed to be undertaken;
 - ii. the types of activities and functions that will be considered for outsourcing;
 - iii. the risks to the firm, which arise from its outsourcing and other third-party arrangements;
 - iv. criteria for the outsourcing of critical or important functions or services; and
 - v. the extent to which the firm has the skills and capacity to monitor and exercise oversight of outsourcing and other third-party arrangements.

Outcome A3 – Roles and Responsibilities

A firm should implement a policy on outsourcing and third-party arrangements that clearly outlines roles and responsibilities within the firm and an agreed third-party risk management approach.

Foundational good practices

- A3.1 A firm should have a policy on outsourcing and third-party arrangements that outlines:
- a) The firm's risk appetite as it relates to outsourcing, and particularly its appetite for ICT outsourcing, to support the provision of critical or important functions;
 - b) Roles and responsibilities within the firm for the oversight and management of outsourcing and third-party risk, including:
 - i. the responsibilities of the governing or management body and the extent of its involvement in providing direction and decisions relating to outsourcing and other third-party arrangements;
 - ii. the responsibilities of business lines and internal control functions with regard to outsourcing and other third-party arrangements;
 - iii. clearly assigning the internal responsibilities for the approval, management, control, and documentation of all contractual arrangements including intragroup service providers to support its critical or important functions;
 - c) The criteria and methodology for the identification and classification of outsourcing and other third-party arrangements as critical or important to the firm; and
 - d) The requirement, notwithstanding any contractual arrangements / agreements entered into, to retain ownership and ensure that the firm remains in control of its operational risks, information security and business continuity throughout the lifecycle of contractual arrangements with service providers.

Supporting good practices

- A3.2 A firm's outsourcing and third-party risk management policy should also outline:

- a) The approach to the identification, assessment, mitigation and management of risks associated with outsourcing and use of third parties;
- b) The approach to initial and ongoing due diligence on third parties and the ongoing management, monitoring and review of outsourced arrangements in place;
- c) The process for approval of new outsourcing arrangements including the defining of the business needs for the services proposed;
- d) The need to establish contracts, written agreements and SLAs;
- e) The firm's policy with regard to sub-outsourcing;
- f) The approach and steps to be taken in identifying and addressing potential conflicts of interest which may arise between the firm and the third parties, particularly in the case of intragroup arrangements;
- g) Details of the outsourcing risk management framework and structures for operational oversight and controls;
- h) The approach to business continuity arrangements as they pertain to the outsourcing arrangements;
- i) The requirement for a documented exit strategy for each outsourcing or other third-party arrangement deemed critical or important;
- j) The termination processes, including consideration of unexpected termination of a third-party arrangement and the necessary contingency arrangements to effect a substitution of a third party or implementation of the exit strategy;
- k) The approach to safeguarding and maintaining the integrity of the firm's data and systems;
- l) The documentation and record keeping requirements in relation to outsourcing and other third-party arrangements.

Outcome A4 – Critical or Important Functions

A firm should have an effective risk-based process and criteria for the assessment of the criticality or importance of the activity or service to be outsourced, whether the outsourcing is to third parties or intragroup.

Foundational good practices

- A4.1 In order to manage outsourcing/third-party risk effectively it is necessary to determine the criticality or importance to the firm of the function, service or activity that is being outsourced or in respect of which a third-party arrangement is being entered into. This should determine the risk management measures that should be adopted to ensure resilience and continuity of operations.

Supporting good practices

- A4.2 A defined methodology for determining the ‘criticality or importance’ of a function should clearly set out the criteria/ factors that are considered in making the determination and the rationale; can be applied consistently across all outsourcing decisions; and considers the nature, scale and complexity of the firm’s business.
- A4.3 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.

B. Due Diligence and Risk Assessment

Outcome B1 – Initial Risk Management

A firm should implement a risk management framework to identify, measure, monitor and manage risks inherent in all outsourced functions.

Foundational good practices

- B1.1 When developing its third-party risk management framework and conducting third-party risk assessments, a firm should conduct risk assessments in respect of any proposed outsourcing or other third-party arrangement prior to entering into such an arrangement.
- B1.2 A firm should ensure that third-party risk assessments are tailored to take account of specific risks, for example:
- i. sub-outsourcing risks;
 - ii. sensitive data risks;
 - iii. concentration risks, including over-dependence on a single or small number of third parties that cannot easily be substituted;
 - iv. offshoring risks;
 - v. step-in risk, which is the risk that a firm may need to ‘step-in’ to provide financial support to a third party in distress or to take over its business operations;
 - vi. business continuity risks and threats to a firm’s operational resilience through its dependence on third parties. 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; and
 - vii. legal, regulatory and reputational risks to which a firm may be exposed in respect of the outsourced services.

Supporting good practices

- B1.3 A firm should 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 and alignment with the firm’s risk management

framework, are reflected in the relevant outsourcing/third-party contracts and SLAs.

- B1.4 A firm should regularly review their outsourcing arrangements, with particular focus on their critical or important arrangements. Such reviews should consider:
- i. whether the nature, scale or complexity of the outsourced function or the risks associated with it have changed since its inception or last review;
 - ii. whether any such changes impact the firm's assessment of the criticality or importance of the function and whether the related risks and controls need to be updated accordingly; and
 - iii. whether there have been any changes in the firm's exposure to concentration risk either directly via its third parties or through the introduction of or changes to sub-outsourcing arrangements.
- B1.5 A firm should review and refresh its risk assessments on a periodic basis.
- B1.6 A risk relating 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 its risk management or internal control functions, a firm should carefully consider the outsourcing risks of such functions and the governing or management body should satisfy itself that there are no significant concerns about the governance, risk management or internal control arrangements.
- B1.7 A firm should maintain adequate oversight of these functions.

Outcome B2 – Initial Due Diligence

A firm should carry out a due diligence review prior to entering into agreements with third parties, proportionate to the risk, criticality and importance of the function to be outsourced.

Foundational good practices

- B2.1 A firm should have a documented process for carrying out due diligence on proposed third-party service providers. A due diligence should focus on the proposed third party's financial stability, its security measures, and its ability to meet contractual obligations including data privacy requirements.
- B2.2 A firm should ensure that the third party has the appropriate authorisation, where required, to perform the service.

- B2.3 A firm should conduct a due diligence review in respect of third parties, that considers the third party's business model, nature, scale, complexity, financial health, ownership and group structure if applicable.
- B2.4 The due diligence review of proposed third parties should include a review of:
- a) whether the third party is a member, or is owned by firms that are members, of the same group. In this context of such intragroup arrangements, consideration should be given to the extent of control or influence which may be exercised by the firm;
 - b) potential conflicts of interest, particularly in the case of intragroup arrangements and a documented process for the resolution of any such conflicts should they arise;
 - c) business reputation – including compliance, complaints and outstanding or potential litigation;
 - d) financial performance;
 - e) cross-border activities;
 - f) ability of the third party to meet its requirements and contractual obligations in relation to service quality and reliability, security and business continuity; in both normal and stressed circumstances for all services contracted, including ICT services;
 - g) design and effectiveness of risk management controls at the third party being at least as strong as the controls utilised by the firm itself (i.e. they should meet the firm's control objectives);
 - h) insurance coverage.

Supporting good practices

- B2.5 Additionally, a firm should consider the following when carrying out a due diligence:
- a) the long-term relationships with third parties that have already been assessed and perform services for the firm;
 - b) compliance with the General Data Protection Regulation (GDPR), Data Protection Acts and other applicable legal and regulatory requirements on data protection;
 - c) whether the third party is authorised by a regulatory authority to provide the service and whether or not the third party is supervised or subject to oversight by regulatory authorities;

- d) capacity of the third party to keep pace with innovation within the market sector;
- e) the effectiveness of risk management and internal controls, including IT and cybersecurity in providing appropriate technical and organisational measures, aligned with the firm's risk management framework, to protect the firm's data;
- f) substitutability of the third party (identifying possible alternative or back-up providers);
- g) potential exposure to concentration risk;
- h) the third party's ability to demonstrate certified adherence to recognised, relevant industry standards;
- i) openness of the third party to negotiating mutually acceptable contractual and SLA provisions;
- j) employment and management of sub-contractors by the third party;
- k) reliance by the prospective third party on and control over sub-contractors;
- l) incident reporting and management programmes;
- m) resilience measures;
- n) track record of the third party in respect of termination arrangements without having an impact on the continuity or quality of operations;
- o) alignment of the risk appetite of the third party with that of the firm to avoid risk appetite or regulatory breaches as a result of a third party 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.

C. Contracting

Outcome C1 – Establishing Clearly Defined Third-Party Agreements

A firm should ensure that third party arrangements are governed by formal contracts or written agreements, containing appropriate provisions and performance requirements, supported by detailed Service Level Agreements.

Foundational good practices

- C1.1 Firms should ensure that unambiguous contracts and service level agreements (SLAs) are established for third party arrangements.
- C1.2 The adherence of third parties, whether external third parties or intragroup providers, to contracts, written agreements and SLAs should be monitored by the firm.
- C1.3 Before entering into any third-party arrangement, a firm should identify and assess potential conflicts of interest that the use of third-party service providers (whether external or intragroup) may cause.

Outcome C2– Contractual Provisions and Termination Rights

A firm should ensure that its contractual arrangements include all appropriate provisions.

Foundational good practices

- C2.1 All third party written agreements should include:
 - a) A complete, unambiguous and detailed definition of the specific services being provided and the start and end dates of the agreement.
 - b) Whether the sub-contracting of a critical or important function, or material parts thereof, is permitted and the conditions under which the sub-contracting is permitted. A firm should ensure that the firm's, and the competent authority's, rights of access and audit apply in the case of any sub-contracting arrangement;

- c) The location(s) where the function will be provided and where relevant data will be stored and processed, including a requirement to notify the firm, in advance, if the third party proposes to change the location(s).
- d) Provisions on data availability, authenticity, integrity and confidentiality. Where third parties are located abroad, the firm should take into account differences in national provisions with respect to data protection, and recovery and/or resolution mechanisms.
- e) Clearly defined and measurable service level descriptions.
- f) The rights of the firm to monitor the third party's performance on an ongoing basis, including full access to all relevant business premises, devices, systems, networks, information and data used for providing the outsourced function.
- g) The obligation of the third party to co-operate with the competent authorities.
- h) Termination rights and notice periods.

C2.2 For third-party agreements covering critical or important functions, firms should include the following terms in written agreements:

- a) The obligations of the third party to provide the firm with timely reporting against key performance indicators (KPIs) and well-defined quantitative and qualitative performance targets.
- b) The requirement for communication by the third party of any development that may have a material impact on the third party's ability to effectively carry out the critical or important function. Timeliness expectations for such notifications to the firm should be defined.
- c) Where sub-contracting critical or important functions, the contract between the firm and the third party should include provisions in respect of:
 - i. The conditions to be complied with by the third party and the sub-contractor.
 - ii. Activities that should be excluded for the sub-contracting arrangement.
 - iii. The obligation of the third party to continuously monitor sub-contractor performance and adherence of the sub-contractor with defined performance standards. Reporting obligations of the sub-contractor should also be defined.

- iv. The obligation of the third party to maintain continuity of critical or important activities, including in the case of the failure of sub-contractors within the supply chain.
- v. The right of access, inspection and audit, as appropriate, by the firm, the third-party and the competent authorities.
- d) The obligation of the third party to cooperate with the competent authorities (and the resolution authority if applicable) including other persons appointed by them, and to provide:
 - 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 third party's external auditors; and;
 - ii. unrestricted rights of inspection and auditing related to the third-party arrangement, to enable the firm or the Central Bank to monitor the arrangement and to ensure compliance with all applicable regulatory and contractual requirements.
- e) The requirement for third parties to implement and regularly test business continuity plans, taking account of the firm's impact tolerances for the disruption of critical or important services.
- f) Exit strategies including defined service transition periods and protocols to reduce disruptions risks and to enable the firm to substitute or re-integrate the outsourced activities.
- g) Provisions that ensure that the data owned by the firm can be accessed and recovered in the case of the insolvency, resolution or discontinuation of business operations of the third party;
- h) Whether the third party should take out mandatory insurance against certain risks and, if applicable, the level of insurance cover required;
- i) The unrestricted right of firms (and the firm's competent authority) to inspect and audit the third party and the obligation of the third party to co-operate with the competent authority during the course of the engagements.

C2.3 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.

Supporting good practices

- C2.4 A firm is expected to exercise its access and audit rights, determine the audit frequency and areas to be audited using a risk-based approach. This should be reflected in the firm's audit plans.
- C2.5 Additional considerations for contractual arrangements should include:
- a) Contractual arrangements should ensure that where a situation of recovery and/or resolution arises it cannot be deemed to be grounds for termination by the third party of outsourcing arrangements in respect of critical or important services;
 - b) The right of the firm to monitor the third party's performance on an ongoing basis by reference to key performance indicators (KPIs) which should be set out in the associated SLA, and the right to take corrective action without undue delay if the KPIs are not met;
 - c) The contract or written agreement should expressly allow the possibility for a firm to terminate the arrangement where instructions to terminate are given by a competent authority, e.g. in the case that the competent authority is, as a consequence of the outsourcing arrangement, no longer in a position to effectively supervise the firm.
 - d) The contract or written agreement governing the outsourcing arrangement should facilitate the transfer of the outsourced function to another third party or its re-incorporation into the firm.

D. Ongoing Risk Management and Monitoring

Outcome D1– Record Keeping

A firm should maintain complete and up-to-date records and register to facilitate oversight of its third-party service provider arrangements.

Foundational good practices

- D1.1 A firm should ensure that it maintains complete and up-to-date records and register of all its third-party service provider arrangements.

D1.2 A firm should identify in its records or register appropriate management information to permit the firm to better manage the risks that may arise, such as:

- a) A unique reference number for each third-party arrangement and the type of contractual arrangement chosen (“Standalone arrangement”, “Overarching arrangement”, or “Subsequent or associated arrangement”; - for the latter option, the reference number of the overarching arrangement should be specified);
- 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 firm;
- 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 firm that reflects the nature of the functions (as described under point c) above) covered by the third-party arrangement which should facilitate the identification of different types of arrangements. If an arrangement covers multiple functions, then a firm should record as many categories as the functions provided;
- e) The name of the third party, the legal entity identifier (LEI, EUID where available), the corporate registration number, the registered address and other relevant contact details, and the name of its ultimate parent company (and LEI, EUID if any) the details should specify whether the third party is a regulated firm and if so, provide the name of the relevant regulator;
- f) The country or countries where the service is to be performed, including the locations (i.e. countries or regions) of data storage, and where it will be processed;
- g) Whether or not (yes/no) the outsourced function is considered critical or important, including, where applicable, a 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 and processed;

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

D1.3 For the outsourcing of critical or important functions, the register should include the above and at least the following additional information:

- j) The date/s of the most recent due diligence and risk assessments conducted including those involving services provided by sub-outsourcing providers and a summary of the main results;
- k) The individual or decision-making body (e.g. the management body) in the firm that approved the outsourcing/third-party arrangement;
- l) The governing law of the outsourcing/third-party contract or agreement;
- m) The dates of the most recent and next scheduled audits and reviews, where applicable - (to include reviews conducted by the firm itself, its internal audit function and/or any independent third-party reviews);
- n) 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, an identifier (LEI, EUID) the type of functions or material part subcontracted, the rank in the chain of the sub-contractor, where the service will be performed and, if applicable, the location (i.e. countries or regions) where the data will be stored and processed;
- o) An outcome of the assessment of the service provider's substitutability including reasoning (as one of the following options: 1. Not substitutable, 2. Highly complex substitutability, 3. Medium complexity in terms of substitutability, 4. Easily substitutable), the possibility of reintegrating a critical or important function into the firm or the impact of discontinuing the critical or important function;
- p) Summary and date of the last assessment performed of the possibility of reintegrating a critical or important function into the firm or the impact of discontinuing the critical or important function together with the recovery time objective of the function and the recovery point objective of the function;
- q) Identification of alternative service providers in line with point p);
- r) Whether the outsourced critical or important function supports business operations that are time-critical;

- s) Confirmation and latest dates of the testing of business continuity plans and exit strategies;
- t) Confirmation and dates of testing of the third party's business continuity plans;
- u) The estimated annual budget cost;
- v) Whether or not the third-party service provider or sub-service provider is part of a group of which the firm is a member, or is owned by firms within the same group; and
- w) The firms within the scope of the prudential consolidation that make use of the third-party service provider (i.e. the details of all the firms/subsidiaries within a group using the service).

Outcome D2– Ongoing Risk Management

Risks arising from dependencies on third-party arrangements are identified, measured, monitored and managed.

Foundational good practices

- D2.1 A firm should put in place appropriate mechanisms to oversee, monitor, and assess the appropriateness and performance of its outsourced and other third-party arrangements.
- D2.2 A firm should take appropriate measures to ensure that any deficiencies identified in the provision of the service by the third party are effectively addressed, and if necessary escalated to ensure remediation. Escalation may include an ultimate decision to terminate the arrangement.

Outcome D3– Management of Key Risks

Firms should take account of specific risks associated with the use of third parties.

Foundational good practices

Sub-Outsourcing (or sub-contracting)

- D3.1 A firm should determine and document its appetite for sub-outsourcing as part of the firm's outsourcing policy and should actively manage the associated risks via its contractual arrangements and monitoring and oversight mechanisms.
- D3.2 Sub-outsourcing risk arising from intragroup arrangements should be treated in the same manner as that with external third parties.
- D3.3 A firm should monitor sub-outsourcing of critical or important functions, or parts thereof, for any exposure to concentration risks related to the sub-outsourced service providers.
- D3.4 A firm should not agree to sub-outsourcing unless the sub-contractor agrees to:
- a) comply with the relevant laws, regulatory requirements and contractual obligations; and
 - b) provide the firm (and the firm's competent authority) the same contractual rights of access and audit as those granted by the primary third party.

Intra-group arrangements

- D3.5 A firm that uses centrally provided governance arrangements and/or centrally provided intragroup critical or important services or functions, should:
- a) apply the same rigour when conducting intra-group outsourcing risk assessments and due diligence as for external third-party assessments
 - b) Consider and be satisfied with the application of the appropriate level of prioritisation of any remediation or restoration of outsourced services, where service outages may impact the firm and/or the wider group;
 - c) Ensure that the arrangements are appropriately at "arms-length" and the resolution of any potential conflicts of interest is provided for in the governance arrangements; and
 - d) Assess if policies and procedures applied at group level are fit for purpose at the local firm and that these policies and procedures comply with the legal and regulatory obligations of the local firm.
- D3.6 Where the operational monitoring of third-party arrangements is centralised (e.g. as part of a master agreement for the monitoring of third-party arrangements at group level), a firm should ensure that for critical or important services provided by third-party service providers, monitoring of the third-party service provider is performed. This should include the receipt of reports that include, at least, the risk assessment and performance monitoring. In addition, a firm should receive from the centralised function a summary of the relevant audit reports for critical

or important functions provided by third-party service providers and, upon request, the full audit report.

- D3.7 A firm should ensure that its governing or management body is duly informed of any relevant planned changes regarding third-party service providers that are monitored centrally and the potential impact of these changes on the critical or important services provided, including a summary of the risk analysis, including legal risks, compliance with regulatory requirements and the impact on service levels, in order for the firm to assess the impact of proposed changes.
- D3.8 Where firms within a group rely on a central pre-contractual analysis of third-party arrangements, each firm should receive a summary of the assessment and ensure that it takes into consideration its specific business model, regulatory requirements and specific risk profile within that group decision-making process.
- D3.9 Where a firm relies on an exit plan, (or recovery and resolution plans) for a critical or important function that has been established at group level, the firm should receive a summary of the plan and be satisfied that the plan could be effectively executed.

Concentration Risk

- D3.10 Concentration risk, at a firm level, can arise where a firm develops a dependency on a single or small number of third parties for the provision of critical or important activities or functions. Other examples of concentration risk include but are not limited to (i) concentrations of multiple services provided by the same third-party service provider; (ii) concentration of services from one or multiple third-party service providers in a single geographic region; or (iii) multiple third-party service providers with a dependency on the same sub-outsourced service provider. Concentration risk can also arise at a systemic level (or broader sectoral level) where there is a dependency on one or more services provided by a single provider or a limited number of providers for a sector or across sectors thus giving rise to problems of substitutability.
- D3.11 Concentration risk arises directly from third-party arrangements and indirectly from any sub-outsourcing arrangements undertaken by the third party. In order to monitor and manage this risk, a firm should:
- a) regularly assess and take measures to recognise and manage:
 - i. overall exposure and reliance on third parties and sub-outsourced service providers (fourth parties); and

- ii. concentration risks at firm or group level, due to multiple arrangements with the same or closely connected service providers or arrangements with third parties;
- b) ensure its risk management framework includes the firm's approach to concentration risk identification, management, and reporting;
- c) ensure that its ability to negotiate and secure robust arrangements with service providers is not hindered, even in scenarios where there are a limited number of third parties to choose from.
- d) include conditions in the outsourcing contract/written agreement that require the prior approval of the firm to sub-outsourcing; and
- e) evaluate elements of concentration 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 the same third party or intra-group service provider;
 - ii. lack of substitutability issue arising from single service provider in the market;
 - iii. multiple number of firms outsourcing to same third party either on a sectoral or system-wide basis;
 - iv. concentration risk arising from sub-outsourcing arrangements; and from outsourcing to offshore jurisdictions.

D.3.12 Firms should take reasonable steps to secure contractual protections appropriate to the nature and risks of the arrangement. Where a firm cannot obtain particular protections, it should assess the resulting residual risk, consider available alternatives and implement proportionate mitigating measures. The adequacy of the firm's approach will depend on factors including the criticality or importance of the service, the availability of alternative providers and the effectiveness of other controls.

Offshoring

D3.13 When considering or engaging in outsourcing to offshore jurisdictions, a firm should evaluate the particular risks associated with countries to which it is planning to outsource activities. A firm should consider taking steps to mitigate the following concerns and/or risks:

- Regulatory environment – the strength and expertise of the financial services regulatory regime in operation in the third party's jurisdiction;

- Supervisibility Risk – firms should not enter into third-party arrangements that impede proper supervision by competent authorities;
- Legal risk – in particular differences in insolvency regimes, trade, tax and employment laws;
- Political climate risk – risk of political agenda and/or instability and potential impacts on the ability of the third party to continue providing the service;
- 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 third party to continue providing the service;
- Cultural or language issues – lack of understanding/misunderstanding of expectations and/or issues arising from the third-party arrangement;
- Time-zones – ability to ensure availability of the relevant third-party personnel to deal with service issues in a timely manner; and
- Employment conditions in offshore jurisdictions – a firm should pay careful attention to taxation issues, labour laws and human rights and consider the impact of their outsourcing on all stakeholders; this includes taking into account the firm’s social and environmental responsibilities.

D3.14 A firm should ensure that contracts for outsourced arrangements, including those which are offshored, stipulate that the firm (and its competent authority) are given access to carry out all necessary quality assurance and supervisory work.

D3.15 A firm should ensure that there are minimum standards in place at the third party in respect of risk appetite that are aligned to the firm’s own risk management expectations and requirements to mitigate reputational risks or regulatory breaches.

D3.16 A firm should ensure that issues identified as part of the country risk assessment are also considered as part of the firm’s disaster recovery/business continuity and substitutability planning.

D3.17 A firm should 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.

Outcome D4– Monitoring

A firm should undertake periodic reviews throughout the lifecycle of a third-party arrangement.

Foundational good practices

- D4.1 The criteria set out in Outcome B2 – Initial Due Diligence - should also be considered, during periodic reviews of due diligence throughout the lifecycle of any contract. A firm should consider conducting due diligence reviews that cover the breadth of operational and financial capacity of the third party to provide and maintain a quality service to the firm. These periodic reviews should include the “financial health” of key third parties, providing critical or important services, over the lifecycle of the contract.
- D4.2 Specifically, a firm should undertake or 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 or rollover date to permit the firm sufficient time to either renegotiate the terms of the contract or undertake an orderly wind down or transfer of the arrangements.
- D4.3 A firm should monitor the performance of the third party, including by:
- i. ensuring receipt of appropriate reports from the third party;
 - ii. assessing the performance of the third party, including using measures agreed and documented in their SLAs e.g. key performance indicators (KPIs), key control indicators (KCIIs), service reviews and reports, outcomes of internal audit or other third-party independent reviews;
 - iii. assessing the adequacy of the third party’s business continuity measures and associated testing and the effectiveness of the integration with those of the firm; and
 - iv. conducting onsite reviews of the third party.
- D4.4 A firm should take appropriate measures to ensure that any deficiencies identified in the provision of the service by the third party are effectively addressed, and if necessary escalated to ensure remediation. Escalation may include an ultimate decision to terminate the arrangement.
- D4.5 A firm should include an assessment of the effective performance of third-party arrangements in its internal audit plan. The internal audit plan should assess:

- i. That the firm's outsourcing and third-party risk management framework is operating effectively and in line with the third-party risk management policy and the firm's risk appetite;
- ii. Whether the third-party risk management 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 firm's methodology for the assessment of "criticality and importance".
- iv. That the firm's outsourcing and third-party risk register is being appropriately maintained to ensure accuracy;
- v. The adequacy and appropriateness of the firm's outsourcing and third-party risk assessment and its conduct of due diligence;
- vi. The effectiveness of the oversight and direction of the governing or management body
- vii. The effectiveness of the firm's monitoring and management of its third-party arrangements; and
- viii. The operation by the third party of the underlying outsourced activities or functions via onsite audits.

Supporting good practices

D4.6 A firm should incorporate assurance testing related to the management and monitoring of outsourcing as part of their risk management and compliance monitoring programmes and should document the rationale and the selected frequency of such reviews in its outsourcing and third-party risk management policy.

D4.7 Where a firm utilises third-party certifications provided by the third party and/or pooled audits, a firm should assess the circumstances in which third-party certifications and pooled audits provide appropriate levels of assurance, in line with their outsourcing and third-party risk management policy and risk assessment. Over time, a firm should not exclusively rely on third-party certifications.

E. Incident and Termination Management

Outcome E1– Termination Risks Are Managed Effectively

A firm should understand exit costs, the arrangements to be initiated and the legal and operational (including timing) risk implications in the event of the termination of third-party arrangements.

Foundational good practices

- E1.1 A firm should understand exit costs, the arrangements to be initiated and the legal and operational (including timing) risk implications in the event of the termination of outsourcing contracts or arrangements, whether with third parties or intra-group.
- E1.2 A firm should ensure that it is able to exit third-party arrangements while endeavouring to minimise disruption to its business activities, without limiting their compliance with regulatory requirements and minimising any detriment to the continuity and quality of the provision of services to clients/customers.
- E1.3 A firm should perform a Business Impact Analysis regarding the risk of the processes, services or activities provided by third-party service providers (including intra-group) becoming unavailable with the aim of identifying the human, technical, time and financial resources required to implement an exit plan. A firm should document its 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, up to and including an exit strategy.
- E1.4 A firm should have a clearly defined and documented exit strategy in place, taking into account criticality and substitutability, that is viable, appropriately planned, and documented and regularly tested.
- E1.5 A firm should assess whether a third party can be substituted. Where substitutability is established, a firm should seek to identify alternate third parties and make appropriate assessments of the measures, timings and costs required to transfer to such alternate providers where an exit plan must be invoked.

- E1.6 A firm should ensure that the exit strategy includes arrangements for reintegration of services within the firm, either where an alternative provider is not available or in cases where reintegration is required by regulation.
- E1.7 A firm should develop 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 in an orderly manner.
- E1.8 A firm should ensure that an exit strategy estimates the timeframe for transfer of service either to an alternative provider, or if necessary, to take the service in-house.
- E1.9 A firm should consider and implement within an exit strategy, contingency arrangements to cover the interim period between invoking an exit strategy and the ultimate transfer.
- E1.10 A firm should ensure appropriate understanding and oversight of the data flows between the firm and the third party, including how to manage any potential interruption of service or downtime to ensure that critical business functions remain available.
- E1.11 A firm should consider the potential for and implications of “step-in risk” materialising in the context of stressed scenarios and 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 third party. Where ‘step-in’ is deemed viable, it should be planned and documented as part of an exit strategy.
- E1.12 A firm should ensure that in the case of intra-group arrangements, where a firm avails of exit plans that have been established at a group level, that the plans are viable and address risks for the firm.
- E1.13 Exit strategies should be periodically reviewed and updated 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.

Supporting good practices

- E1.14 When entering into a third-party arrangement, a firm should consider and plan how it would exit the arrangement for example in the case of:

- a) failure on the part of the third party to provide the service to the requisite contracted standard;
- b) unexpected termination of the arrangement dictated by the third party;
- c) stressed circumstances on the part of the third party such as hostile takeover, insolvency or liquidation; and
- d) any other circumstance that the firm envisages may prompt it to exit the arrangement.

Outcome E2– Maintaining Effective Disaster Recovery and Business Continuity Plans

A firm should address risks posed by dependence on third parties and ensure the resilience of the firm's own services.

Foundational good practices

- E2.1 Firms should regularly assess their business processes, disaster recovery (DR) and business continuity plans (BCPs) to ensure that controls or other resilience measures are effective and in line with evolving practices and emerging risks and/or issues.
- E2.2 It is important that there is close alignment of the DR/BCP arrangements of firms and those of the third-party service providers.

Supporting good practices

- E2.3 To ensure resilience and/or the orderly resolution of a firm it is important that the planning of DR/BCP, exit strategies and recovery and resolution measures be undertaken in a holistic and coordinated fashion.
- E2.4 When designing and implementing DR/BCP measures as they pertain to or include outsourced/third-party arrangements, a firm should:
 - a) Ensure that the ability to recover from outages to services of a third party are aligned to 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 BCPs and exit

strategies are updated to reflect any implications of the outsourcing arrangement;

- c) Document and implement BCPs in relation to its critical or 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 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 third party 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.

Outcome E3– Effective Testing of Incident and Termination Plans

Exit strategies, contingencies and termination plans exist and are tested periodically by a firm.

Foundational good practices

E3.1 A firm should:

- a) Regularly review the appropriateness of their business continuity plans and resilience measures in respect of outsourced activities and other third-party arrangements, particularly in the context of new and evolving technologies, trends and risks;
- b) Ensure that any critical or important outsourcing or other third-party arrangement includes a requirement for the third-party service provider to carry out testing of its own business continuity plans at least annually;
- c) Ensure that they can participate in the third party’s business continuity plan testing, where necessary;
- d) Conduct coordinated testing of these arrangements on a regular basis and report the results to the governing or management body of both the firm and the third party;
- e) Have sight of reports on business continuity measures and testing undertaken by the third party and are informed of any relevant actions or remediation arising from this testing, as appropriate; and

- f) Ensure that governing or management body and senior management of the firm take remedial action to address any deficiencies identified in the performance of the third party, either as part of a coordinated testing of the firm's business continuity measures, or via results of the third party's own BCP testing.

Outcome E4– Effective Data Stewardship

A firm should implement effective measures for the appropriate storage, processing, management, retention and destruction of sensitive data.

Foundational good practices

- E4.1 A firm should implement appropriate measures to secure and protect its data and to set out these measures in the firm's third-party risk management policy and the contracts/written agreements governing outsourcing and other third-party arrangements particularly for critical or important functions or services.
- E4.2 A firm should 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, processing and storage including when offshored, which may give rise to heightened data protection concerns.
- E4.3 A firm should give due consideration when conducting risk assessments to the data characteristics of confidentiality, integrity, availability and authenticity of data and information required to deliver outsourced business or service functions.
- E4.4 A firm should design a comprehensive security architecture, the implementation of which may fall to both the firm and the third party.
- E4.5 When considering back-up arrangements a firm should consider the measures necessary to ensure that business critical data is ring-fenced offline and protected against corruption.
- E4.6 A firm should ensure implementation of appropriately designed and operationally effective controls for data, be that data-in-transit, data-in-memory and data-at-rest whether the controls are implemented by the firm or the third party on the firm's behalf.

Supporting good practices

E4.7 A data management strategy should:

- i. define an approach to data security and management, which ensures consistency of application by both the firm and the third party (e.g. “shared responsibility model” in the context of cloud outsourcing);
- ii. address, in terms of location, data at rest, data in memory and data in transit;
- 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 firm’s data including back-up and recovery, security protocols and encryption standards, including key management, access management and legal requirements;
- v. ensure that, where data is encrypted, firms make provisions to guarantee that any encryption keys or other forms of authentication are kept secure and accessible to the firm and to a competent authority; and
- vi. assess and document the risks in respect of any multi-tenanted environment and the implications arising for monitoring and management of the arrangement.

E4.8 A firm should have regard to the requirements of relevant available guidelines or best practice frameworks in the context of information and data security from both a physical and logical perspective.

E4.9 A firm should 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.

E4.10 Regarding the design of security architectures, and especially for cloud services, a firm should ensure consistency of application of security measures both on its own premises and in the cloud. In order to meet this control objective, a firm needs 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);

- iii. platform as a service (PaaS); and/or
- iv. disaster recovery as a service (DRaaS).

E4.11 A firm should additionally consider the following when implementing effective controls for data:

- 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, response and reporting;
- f) Loss prevention and recovery;
- g) Data segregation (if using a multi-tenant environment);
- h) Operating system, network and firewall configuration;
- i) Staff training;
- j) The ongoing monitoring of the effectiveness of the third party’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 a firm’s information security and respond to these incidents appropriately;
- l) Procedures for the deletion of a firm’s data from all the locations where the third party may have stored it following an exit or termination;
- m) Contractual rights to audit the third-party data storage and management systems.

