JULY 2024

REGCOUNSEL FINANCIAL SERVICES WHITE PAPER SERIES #3

Third Party ICT Policy requirements under DORA

ABOUT THE AUTHORS

Mr. dr. drs. Jan Jans is a Dutch qualified lawyer specialized in financial regulatory law. He has a strong focus on the regulatory framework covering investment firms, banks, insurance companies, payment service providers, crypto-asset service providers and investment funds. Prior to joining Regulatory Counsel | Financial Services as Partner in 2022, Jan worked as a financial regulatory lawyer at various (international) law firms in the Netherlands.

Jan graduated from Nijmegen University in 2008. In addition to law, he studied financial economics and business administration. He completed the post-academic education Securities Law at the Grotius Academy in 2012. Jan publishes regularly in national law journals and successfully defended his PhD thesis on the level playing field between banks and non-banks in the European market for electronic payments in 2023.

Prof. dr. Bart Joosen, is professor of Financial Supervision Law at Leiden University. He is also fellow of the European Banking Institute, Frankfurt, Germany. He is member of faculty at the Florence School of Banking and Finance, Italy at the European University Institute. He has expertise on financial services supervision with a focus on micro-prudential supervision of banks, investment firms and payment services providers (including in-depth Basel I-IV, IFR/IFD and Solvency II knowledge). He is an expert in derivatives transactions, repos, securities lending and (synthetic) securitisations.

Mr. drs. Jan-Jouke van der Meer is a Dutch qualified lawyer specialized in financial regulatory law. He advises clients on the full range of Dutch and EU financial regulatory laws (including MiFID, AIFMD, MiCAR, PSD2 and DORA), licensing issues, corporate governance (including integrity and suitability assessments), compliance and integrity-related issues (including AML and sanctions) and dealing with financial regulators. Prior to joining Regulatory Counsel | Financial Services as Managing Associate, Jan-Jouke worked as a financial regulatory lawyer at an international law firm in the Netherlands.

Jan-Jouke obtained a master's degree (LLM) in Corporate Law from VU Amsterdam in 2018, and holds a master's degree (MSc) in Financial Economics from Erasmus University Rotterdam (2018). He has also published various articles in the area of financial regulatory law.

Mr. Maarten Mol-Huging is a Dutch qualified lawyer specialized in financial regulatory law. He advises on (prudential) regulatory issues with regards to banks, investment firms, insurers, crypto-asset service providers and other financial sector entities.

Maarten graduated with distinction from the prudential regulation oriented EBI Master in Banking Regulation in 2024. Before, he graduated cum laude at the VU Amsterdam in International Business Law in 2022 on his thesis titled: The Biggest Challenge yet for EU Mortgage Lending: The Onset of Artificial Intelligence Tooling.

Recofise is a boutique law firm located in Amsterdam and specialises in financial regulation. Our clients consists of financial undertakings (e.g., banks, investment firms and funds, insurance companies, electronic money institutions, payment institutions and crypto-asset service providers) that are active on the Dutch and international financial markets. Recofise has extensive experience in advising and supporting clients with complex legal issues regarding prudential requirements, compliance, risk management, supervisory reporting and supervisory audits.

EXECUTIVE SUMMARY

In view of the growing impact of digital technology on financial services, the European legislature introduced DORA, a landmark regulatory framework aimed at strengthening the operational resilience of entities that are active in the financial sector. One of the main requirements imposed under DORA is the requirement for Financial Entities to adopt a strategy, policies and procedures on third party ICT risk as part of their ICT risk management framework. The background thereof lies in the financial sector becoming increasingly dependent on third parties for the provision of ICT services, in numerous areas. Whilst such third party ICT services offer benefits like efficiency and scalability, they also bring various risks to Financial Entities, particularly to operational resilience, information security, and data integrity.

Recognizing this, DORA – and more specifically the RTS specifying further rules in that respect – requires Financial Entities to have a TP ICT Policy, emphasizing a structured approach to managing third party ICT risks. This policy should define requirements, principles, responsibilities, and processes for each phase of the ICT services lifecycle, including amongst others (a) management responsibilities, (b) contractual planning, (c) business unit involvement, (d) implementation and monitoring, (e) record-keeping and documentation and (f) exit strategies.

A key aspect of DORA in respect of the TP ICT Policy is its focus on governance. Financial Entities are required to establish a governance framework with clear responsibilities for managing and overseeing ICT third-party risk. This includes developing and regularly reviewing the ICT third-party risk strategy, integrating it into the Financial Entity's overall risk management framework. The TP ICT Policy should be reviewed on an annual basis and be updated where necessary, e.g., in the event of significant changes in the ICT landscape or operational environment.

Before signing contracts with ICT third-party service providers, Financial Entities must conduct thorough risk assessments. This includes assessing the impact of ICT services on the entity's overall risk landscape, covering operational, legal, ICT-related, reputational, and data protection risks. Considerations should also include data availability, data processing and storage locations, and the geographic location of the ICT service provider. The assessment should also address concentration risks, i.e., to prevent over-reliance on a limited number of ICT service providers.

Moreover, a comprehensive due diligence process is essential to scrutinize contractual arrangements with prospective ICT third-party service providers, ensuring they meet regulatory and operational requirements. For this purpose, before entering into a contractual arrangement, the Financial Entity should assess whether the ICT third-party service provider, *inter alia*, (i) has sufficient expertise to provide the ICT services, (ii) intends to use ICT sub-contractors, (iii) is located in a third country, (iv) allows audits by the Financial Entity, and (v) acts in an ethical and socially responsible manner.

The RTS require stringent documentation and reporting of the ICT third-party risk management process. Financial Entities must maintain a detailed register of all contractual arrangements with ICT third-party service providers. This documentation is vital for transparency and accountability, allowing supervisory authorities to monitor the Financial Entity's ICT third-party risk profile effectively.

The RTS also mandate that the TP ICT Policy must include ongoing monitoring strategies and metrics to evaluate provider performance. This includes mechanisms to ensure adherence to standards for data confidentiality, availability, integrity and authenticity, and compliance with the Financial Entity's policies. The TP ICT Policy should also detail actions for addressing breaches of service level agreements, including contractual penalties if necessary.

A critical component of the RTS is that it requires Financial Entities to devise exit strategies for their ICT third-party service contracts. These strategies should include, e.g., clear protocols for transitioning to alternative providers or bringing services in-house, without disrupting critical functions. This proactive approach is vital for maintaining operational continuity and resilience.

To ensure compliance with the extensive TP ICT Policy requirements under DORA, we recommend Financial Entities to consider, *inter alia*, taking the following steps:

- Conduct a gap analysis of their current policy framework against the TP ICT Policy requirements and map out the extent to which their current policy framework falls short;
- Identify which ICT services third parties (including intra-group entities) provide to them;
- Decide whether they should draft a new TP ICT Policy or can incorporate the TP ICT Policy requirements into their current policy framework, also taking into account the group application requirements (i.e., should the Financial Entity rely on a group-wide TP ICT Policy, or should they draft an individual TP ICT Policy) and operational environment;
- Draft a new TP ICT Policy or incorporate the TP ICT Policy requirements into their current policy framework, taking into account how compliance with the requirements can be best achieved from an operational perspective; and
- Draft a standard "DORA addendum".

TABLE OF CONTENTS

1.
INTRODUCTION

1. INTRODUCTION

Given that financial entities are becoming more and more dependent on information and communication technology ("**ICT**") for the offering of financial services, financial entities see themselves increasingly exposed to ICT-related risks. With the Digital Operational Resilience Act ("**DORA**")[1], the European legislature aims to address these concerns by requiring that financial entities uphold rigorous policies and procedures concerning their ICT security. DORA forms part of the broader Digital Finance package[2] of the European Commission ("**Commission**") and seeks to bring harmonisation of the rules relating to operational resilience for the financial sector applying to not fewer than 20 different regulated and unregulated financial entities (each of which hereinafter referred to as: "**Financial Entity**").[3]

Given that DORA will apply from 17 January 2025, compliance with its comprehensive requirements becomes more and more urgent. One of the main requirements imposed under DORA is the requirement for Financial Entities to adopt a strategy, policies and procedures on third party ICT risk as part of their ICT risk management framework. The background is that the financial sector has become increasingly dependent on third parties for the provision of ICT services, in numerous areas. DORA provides a far-reaching framework to bound the risks associated with this dependency. This strategy must include a policy on the contractual arrangements regarding the use of ICT services supporting critical or important functions of financial institutions ("**CIFs**") provided by ICT third-party service providers (the "**TP ICT Policy**"). Whilst policies covering similar requirements have already to a certain extent been adopted by most Financial Entities under the current legislative framework, DORA requires Financial Entities to conduct a thorough review and revision of their third-party risk governance.

1 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

2 Commission: *Digital Finance Package: Commission sets out new, ambitious approach to encourage responsible innovation to benefit consumers and businesses,* (link).

3 DORA applies to the following financial undertakings (i) credit institutions, (ii) payment institutions (whether subject to authorisation requirements or not), (iii) electronic money institutions (whether subject to authorisation requirements or not), (iv) investment firms, (v) crypto-asset service providers and issuers of asset-referenced tokens, (vi) central securities depositories, (vii) central counterparties, (viii) trading venues, (ix) trade repositories, (x) managers of alternative investment funds, (xi) UCIT management companies, (xii) data reporting service providers, (xiii) insurance and reinsurance undertakings, (xiv) insurance intermediaries, (xv) reinsurance intermediaries and ancillary insurance intermediaries, (xvi) institutions for occupational retirement provisions, (xvii) credit rating agencies, (xviii) administrators of critical benchmarks, (xix) crowdfunding service providers, and (xx) securitisation repositories. DORA does however not apply to (a) managers of alternative investment funds as referred to in Article 3(2) of Directive 2011/61/EU (generally referred to as AIMD Light Managers not subject to authorisation), (b) insurance and reinsurance undertakings as referred to in Article 4 of Directive 2009/138/EC (being insurance undertakings not subject to Solvency II in view of the low premium volume or technical provisions staying below certain thresholds), (c) institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total, (d) natural or legal persons exempted pursuant to Articles 2 and 3 of Directive 2014/65/EU, (e) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises or small or medium-sized enterprises, (f) post office giro institutions as referred to in Article 2(5), point (3), of Directive 2013/36/EU.

This White Paper covers an in-depth review of the new framework applicable to the TP ICT Policy under DORA, referencing, where possible, relevant (draft) legislation. Moreover, this White Paper contains comparisons of the rules currently applied by the European Supervisory Authorities ("**ESAs**") to outsourcing ICT services to third parties, such as the EBA Guidelines on outsourcing arrangements[4] ("**EBA Guidelines**") and the ESMA Guidelines on outsourcing to cloud service providers[5] ("**ESMA Guidelines**", together with the EBA Guidelines: "**Current ESA Outsourcing Guidelines**"). In this regard it is important to note that contrary to the Current ESA Outsourcing Guidelines, DORA will apply to all ICT contractual arrangements entered into by Financial Entities and not only those that qualify as 'outsourcing'. Furthermore, DORA does not provide for a different approach between existing and new ICT contracts, meaning that Financial Entities must ensure that all their contractual ICT arrangements are adapted in order to comply with DORA as of 17 January 2025.

The details of the requirements that are to be covered in the TP ICT Policy are set out in the Delegated Regulation on the policy regarding contractual arrangements ("**RTS**").[6] The RTS have been adopted on 13 March 2024 by the Commission and were published in the Official Journal on 25 June 2024. The RTS set out the minimum requirements that must be covered by the TP ICT Policy in respect of ICT third-party services supporting CIFs, including aspects such as governance, risk management and contractual requirements. The RTS will be discussed extensively in this White Paper, touching on key-focus points for Financial Entities, taking into account the principle of proportionality as enshrined in the DORA framework to address the consequences of application of DORA rules on the various types of Financial Entities and different risk profiles they may present.

4 EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02.

5 ESMA Guidelines on outsourcing to cloud service providers, ESMA50-157-2403.

6 Commission Delegated Regulation (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers, OJEU 2024/1773.

2.
DORA IN A NUTSHELL

2. DORA IN A NUTSHELL

2.1 Background

DORA aims to foster innovation and competition in digital finance while effectively addressing associated ICT risks.[7] The pervasive use of ICT in the financial sector and ever increasing digitalisation of finance necessitates direct attention to these risks rather than treating them as secondary to business processes.[8] This integration extends across a wide range of financial services offered both in the retail markets as in the wholesale markets, from payments, electronic money issue and distribution, (consumer) credit to clearing, settlement and (algorithmic) trading.[9]

Moreover, ICT risks present a persistent challenge to the operational resilience and stability of the European financial system.[10] Previous approaches to addressing these risks, dating back to the 2008 financial crisis, have been indirect and judged insufficient in ensuring digital operational resilience.[11] One of the reasons for such inadequacy is the existing patchwork of both European and national regulation in respect of ICT risks. Such a disperse regulatory framework exacerbates operational challenges for Financial Entities, increasing their compliance and risk management costs, particularly where they operate on a cross-border or cross-service basis. With DORA, the European Union aims to put an end to the existing (sectoral) fragmentation of (operational) ICT risk management and cybersecurity rules and uncoordinated initiatives in the financial sector as developed in the different Member States of the European Union ("**EU**").[12]

Against this background, the Commission published a proposal for DORA on 24 September 2020, providing for a new regulation entirely dedicated to cybersecurity in the financial sector, providing for a lex specialis of the more general Network and Information Systems Directive ("**NIS2 Directive**") which applies to a wider community of businesses and sectors in the EU.[13] The EC's intention with DORA was to provide a tailor-made solution that could be directly

7 Proposal for DORA by the European Commission, p. 2.

8 Recital 2 DORA; see for a stock take of the digitalisation of banking, Basel Committee on Banking Supervision, *Digitalisation of finance*, (2024).

9 Ibid.

10 Recital 5 DORA.

11 Ibid.

12 Recital 12 DORA.

13 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.

applied to the vast majority of the financial sector, using maximum harmonisation instead of the NIS2 Directive that can be subject to national implementation differences and does not cover the same Financial Entities. The DORA package consists of the Regulation itself (Level 1), regulatory and implementing technical standards (Level 2) and supervisory guidance (Level 3). The development of the substantial suite of technical standards and supervisory guidance has been divided into two (2) batches. The first batch was submitted by the ESAs to the Commission for adoption in January 2024 and comprised, among others, the RTS which are the subject matter of this White Paper. The second batch was open for public consultation until 4 March 2024, and must be submitted to the Commission by 17 July 2024.

2.2 Scope

To achieve a common level of digital operational resilience in the EU, DORA lays down uniform requirements concerning the security of network and information systems supporting the business processes of a large variety of different entities that are active in the financial sector. The scope of DORA is broader than that of the Current ESA Outsourcing Guidelines and other frameworks governing the businesses concerned (for instance the separate rules applicable to central counterparties subject to the elaborate regime pursuant to EMIR[14]) as it also applies to, *inter alia*, (i) account information service providers, (ii) exempt payment institutions and electronic money institutions, (iii) insurance, reinsurance and ancillary insurance intermediaries, (iv) crypto-asset service providers, and (v) crowdfunding services providers.

Moreover, DORA does not only apply to contractual relations that qualify as outsourcing under the Current ESA Outsourcing Guidelines, it covers all service relations with ICT third-party service providers ("**ICT TPSPs**"), being those undertakings that provide ICT services to Financial Entities. Given that the scope of applicability is very broad, it is essential to understand what is to be understood as an ICT service under DORA.

14 Regulation (EU) No 648/2012.

ICT services are digital and data services provided through ICT systems to one or more internal or external user(s) on an ongoing basis, including hardware as a service and hardware services, which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services.[15] Thus, as a general rule, the following services are considered ICT services:

- Hardware procurement, maintenance and replacement planning (servers, workspace and desktop equipment);
- Application architecture design, procurement, management, upgrading and lifecycle planning;
- Software development, custom design and management, Software as a Service (SaaS), software platform, IT consulting, customer relationship management systems, website design and development, mobile app design and development;
- Database design, management and maintenance;
- Data storage management services, including private or public cloud solutions, data lakes and warehouses;
- Big data management, data analytics, data integration tools, artificial intelligence applications development, management and maintenance;
- Data and cyber security systems design, management and maintenance, including tokenisation of data, end-to-end encryption processes;
- Network design, management and maintenance, including offline or online remote access work spaces for employees;
- Computing platform design, management and maintenance (including Infrastructure as a Service (IaaS), Platform-as-a-Service (PaaS));
- Communication design, management and maintenance (data lines, telephone, VoIP, etc.);
- Threat protection design, management and maintenance, including business continuity services, disaster recovery services, data vaults design, management and maintenance.

15 Art. 3(20)-(21) DORA.

2.3 DORA pillars

In general, DORA consists of five (5) different pillars:[16]

I **ICT risk management requirements:** DORA imposes requirements that require Financial Entities to establish processes and systems to adapt to the rapidly changing cyber threat landscape. These measures aim to minimize the impact of ICT risks by continuously identifying them from various sources and addressing them through internal controls, disaster recovery plans, and measures to protect the integrity, safety, and resilience of ICT systems and supporting physical infrastructures.

II **ICT-related incident reporting:** DORA mandates the establishment of effective processes for monitoring, handling, and following up on ICT-related incidents. This includes identifying and eliminating root causes to prevent their recurrence.

III **Digital operational resilience testing:** This involves periodically assessing capabilities and functions within the ICT risk management framework to identify weaknesses, deficiencies, and gaps. Corrective measures are then implemented, with particular emphasis on so-called threat-led penetration testing ("**TLPT**"), which enables Financial Entities to conduct penetration testing based on the specific threats they face.

IV **ICT third-party risk management:** As reliance on ICT TPSPs increases, Financial Entities must manage these relationships throughout their lifecycle, from contracting to termination and post-contractual stages, following the minimum requirements outlined in DORA.

V **Information sharing:** Additionally, to foster awareness and growth, DORA allows for information sharing agreements among Financial Entities.

This White Paper focuses on DORA's policy requirements for the contractual arrangements surrounding the use of ICT services supporting CIFs provided by ICT TPSPs, which, in terms of the above, primarily falls under Pillar IV: ICT third-party risk management. It is particularly the ICT services provided by ICT TPSPs that support CIFs that are subject to the governance requirements for ICT third-party risk management under DORA and the RTS.

16 Where we do not take into account the oversight framework for critical ICT TPSPs of art. 31 *et seq.* DORA as this is not directly relevant for Financial Entities.

The definition of CIFs included in DORA is rather broad,[17] and means 'a function, the disruption of which would materially *impair the financial performance of a Financial Entity*, or *the soundness or continuity of its services and activities*, *or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a Financial Entity with the conditions and obligations of its authorisation*[18], or with its other obligations under applicable financial services law'.[19] By applying such broad definition, the European legislature (intentionally) provided for a principle-based definition of CIFs, which allows the market some flexibility and granularity in assessing whether a particular function qualifies as a CIF. As the ESAs consciously chose not to provide further guidance regarding the interpretation of the definition of CIFs, Financial Entities will have to perform a case-by-case assessment whether it considers a particular function to be critical or important.[20]

Recital (70) of DORA indicates that the definition of CIFs provided for in DORA encompasses the "critical functions" as defined under the Bank Recovery and Resolution Directive ("**BRRD**"). The BRRD qualifies critical functions as '*activities, services or operations the discontinuance of which is likely in one or more Member States, to lead to the disruption of services that are essential to the real economy or to disrupt financial stability due to the size, market share, external and internal interconnectedness, complexity or cross-border activities of an institution or group, with particular regard to the substitutability of those activities, services or operations*'.[21] The concept of a critical function has been further specified in Delegated Regulation (EU) 2016/778 ("**BRRD Delegated Regulation**")[22], which states that a function is critical if it fulfils both of the following elements:

17 Art. 3(22) DORA.

18 The reference to authorisation requirements is problematic in case the Financial Entity concerned is not subject to authorisation requirements, such as exempt payment institutions or exempt electronic money institutions. These exempt institutions are also subject to the DORA requirements, but it is unclear against which compliance framework such Financial Entities must test their operational resilience.

19 Art. 3(22) DORA.

20 ESA, *Consultation Paper on Draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554*, (2023), p. 21: *'Specifications to the definition [of CIF] would lead to a higher level of harmonization. However, a too specific definition would create the risk that it leaves out some aspects that might become more relevant over time. In addition, considering the different types of financial entities that are subject to DORA, relying on the definition within DORA, without the provision of detailed specifications seems to be more appropriate.'*

21 Art. 2(1)(35) BRRD.

22 Commission Delegated Regulation (EU) 2016/778 of 2 February 2016 supplementing Directive 2014/59/EU of the European Parliament and of the Council with regard to the circumstances and conditions under which the payment of extraordinary ex post contributions may be partially or entirely deferred, and on the criteria for the determination of the activities, services and operations with regard to critical functions, and for the determination of the business lines and associated services with regard to core business lines.

I the function is provided by an institution to third parties not affiliated to the institution or group; and

II the sudden disruption of that function would likely have a material negative impact on the third parties, give rise to contagion or undermine the general confidence of market participants due to the systemic relevance of the function for the third parties and the systemic relevance of the institution or group in providing the function.

By way of comparison, the definition of CIF under the EBA Guidelines is based on the definition applied under Directive 2014/565 (**MiFID II**)[23] and as further detailed in art. 30 of Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II: '*an operational function shall be regarded as critical or important where a defect or failure in its performance would materially impair the continuing compliance of an investment firm with the conditions and obligations of its authorisation or its other obligations under [MiFID II], or its financial performance, or the soundness of the continuity of its investment services and activities*'. As can be seen, this definition is closely aligned with that of CIFs under DORA.

23 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.

3.
GENERAL REMARKS ON THE TP ICT POLICY

3. GENERAL REMARKS ON THE TP ICT POLICY

3.1 Legal framework

Under DORA, Financial Entities are required to manage ICT third-party risk as an integral component of ICT risk within their larger ICT risk management framework. As part of their ICT risk management framework, Financial Entities must in principle adopt, and regularly review, a strategy on ICT third-party risk.[24] Said strategy must cover the TP ICT Policy and should apply on an individual basis and, where relevant, on a sub-consolidated and consolidated basis.

3.2 Group application

We note that the requirements set out under the RTS are applicable to EU Financial Entities (including parent undertakings in the EU, where applicable).[25] The parent undertaking, if located in the EU, that is responsible for the financial consolidation must supervise the consistent implementation and effective application of the RTS by the Financial Entities is the group. The application at group level does not apply to parent undertakings outside of the EU. Though the initial draft by the ESAs seemed to indicate a broader application, the final RTS as published in the Official Journal only refer to Financial Entities, which have been defined in art. 2(2) DORA as entities authorised to provide financial services in the EU. It appears therefore, that the Commission deviated from the wording of the ESAs which used the term *subsidiary*, limiting the application of the RTS to the Financial Entities included in the group and listed in art. 2(1)(a) to (t) DORA. In doing so, the RTS now seem to exclude any entities located in third countries that would have qualified as Financial Entities had they been located in the EU or any EU non-financial entities included in the group. For the avoidance of doubt, the RTS itself apply to contractual arrangements on the use of ICT services supporting CIFs wherever those ICT TPSPs are located.

24 Art. 28(2) DORA.
25 Art. 2 RTS.

The requirement included in art. 2 RTS resembles the requirement under the EBA Guidelines, which guidelines apply on a sub-consolidated and consolidated basis, taking into account the prudential scope of *consolidation*.[26] Where the RTS refer to groups, we consider it to be the better view that consolidation here means financial consolidation within the meaning of the Accounting Directive.[27] As such, groups that are subject to financial consolidation are required to apply DORA on a consolidated level. It appears that the parent undertaking responsible for the group application of the Policy does not have to be a Financial Entity itself. The term *parent undertaking* is defined in art. 3(27) DORA solely with a reference to the financial consolidation scope, not referring to the definition of Financial Entity.

It would seem intuitive for large groups of companies to apply a group-wide TP ICT Policy in this respect. According to the ESAs, a group-wide TP ICT Policy, adopted by the Financial Entities within the group, is indeed possible. However, such policy should take into account the specificities at (each) individual level, and ensure that, at all times, the individual Financial Entities remain responsible to comply with the obligations under DORA and the RTS at individual level.[28] The parent undertaking, where applicable, is responsible at group level to ensure a consistent and well-integrated implementation of group-wide arrangements. The responsibility for the implementation of local policy then belongs to the local Financial Entity. That being said, the requirements do not prevent Financial Entities and groups to implement the TP ICT policy as appropriate and in a manner that leverages on a parent level and takes into account local level specificities.

It is important to note that in groups where different types of Financial Entities are consolidated, alignment issues between the applicable regulation for one entity may make the consolidated application of the TP ICT Policy difficult for other entities. Financial Entities should therefore properly account for the group structure in the TP ICT Policy. Additionally, it is of key importance to recognise that in principle, the outsourcing policy of Financial Entities is not necessarily aligned to the DORA policy requirements and thus that two (2) policy documents theoretically must exist in parallel to each other. Nevertheless, in our view, it is best for Financial

26 EBA Guidelines, para. 21.

27 Directive (EU) 2013/34 of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC.

28 Final Report on draft RTS, p. 34.

Entities to amalgamate the outsourcing policy and the TP ICT Policy into a single, comprehensive policy document, capturing both CIFs offered by third party ICT providers where there is also question of outsourcing and those services that do not qualify as such (for the latter one could think of hardware maintenance). Thus, the initial scoping of the governance of the TP ICT Policy will have a pivotal role in the embedding of the DORA requirements in the prudent business organisation of Financial Entities.

The Financial Entity's TP ICT Policy on the use of ICT TPSPs, including ICT intragroup providers, should define crucial parts of the Financial Entity' governance arrangements, risk management and internal control framework with regard to the use of ICT services provided by ICT TPSPs and should ensure that the Financial Entity remains in control of its operational risks, information security and business continuity (including disaster recovery methods) throughout the life cycle of contractual arrangements with such providers. To ensure a consistent and uniform application by Financial Entities across the EU, the content of the TP ICT Policy has been further specified in the RTS. The relevant elements of this RTS have been set out in more detail below.

3.3 Guiding principles

In drafting the ICT TPSP risk management framework, Financial Entities must act in accordance with the following principles:

a. Financial Entities that have in place contractual arrangements for the use of ICT services to run their business operations must, at all times, remain fully responsible for compliance with, and the discharge of, all obligations under DORA and applicable law;

b. Financial Entities' management of ICT third-party risk must be implemented in light of the principle of proportionality, taking into account:

   I. the nature, scale, complexity and importance of ICT-related dependencies;

   II. the risks arising from contractual arrangements on the use of ICT services concluded with ICT TPSPs, taking into account the criticality or importance of the respective service, process or function, and the potential impact on the continuity and availability of financial services and activities, at individual and at group level.

3.4 Proportionality principle

Zooming in on the proportionality principle, a similar line of reasoning as required under the Current ESA Outsourcing Guidelines could be employed, where the Financial Entities identify the level of importance, or criticality, of services offered by a ICT TPSP and apply the risk management requirements accordingly. More critical ICT TPSPs should be subject to thorough and comprehensive risk assessments, whereas less relevant ICT TPSPs, still supporting CIFs, could be subject to a less intensive process, perhaps even leveraging standard or framework documentation. When drafting its ICT TPSP risk management framework, a Financial Entity should take good note of such proportional arrangements in order to reduce the operational load where possible.

The principle of proportionality is primarily engraved in art. 4 DORA, which stipulates that the application of Chapter V Section I of DORA (i.e., the Chapter and Section under which the TP ICT Policy falls) by Financial Entities must be proportionate to their size, and overall risk profile, and to the nature, scale and complexity of their activities. In this regard, the RTS repeat the importance of the application of proportionality in the TP ICT Policy and they provide further specific criteria that can be taken into consideration by Financial Entities for a proportional application of the TP ICT Policy.[29] These criteria are non-exhaustive and Financial Entities can also develop their own criteria. However, Financial Entities should in any event be able to demonstrate to their competent authorities that their own proportionality considerations are relevant criteria. The RTS should in our view nevertheless be interpreted as providing for a non-exhaustive list of criteria to be considered by Financial Entities for the application of the principle of proportionality.

The principle of proportionality as applied under DORA resembles the same principle of proportionality that is used in the Current ESA Outsourcing Guidelines.[30] When focusing on DORA, we note that the criteria to be taken into account in respect of proportionality appear to be more focused on the position and circumstances of the third party (i.e., the ICT TPSP) rather than on the circumstances of the Financial Entity itself. When construed in such a way, the principle of proportionality represents a form of initial risk-assessment performed by the European legislature as to what circumstances pertaining to the ICT TPSP

29 Recital (3) and art. 1 RTS.
30 EBA Guidelines, para. 18.

may be seen as risk mitigating and thus warranting a proportional approach. Art. 1 RTS namely stipulates that Financial Entities, when drafting their TP ICT Policy, must ensure that the TP ICT Policy takes into account at least the following elements of increased or reduced risk or complexity:

a. the type of ICT services included in the contractual arrangement on the use of ICT services supporting CIFs provided by ICT TPSPs between the Financial Entity and the ICT TPSP;

b. the location of the ICT TPSP or the location of its parent company;

c. whether the ICT services supporting CIFs are provided by an ICT TPSP located within a Member State or in a third country, also considering the location from where the ICT services are provided and the location where the data is processed and stored;

d. the nature of the data shared with the ICT TPSP;

e. whether the ICT TPSP is part of the same group as the Financial Entity to which the services are provided;

f. the use of ICT TPSP that are authorised, registered or subject to supervision or oversight by a competent authority in a Member State or subject to the oversight framework under Chapter V, Section II, of DORA, and the use of ICT TPSP that are not;

g. the use of ICT TPSPs that are authorised, registered or subject to supervision or oversight by a supervisory authority in a third country, and the use of ICT TPSPs that are not;

h. whether the provision of ICT services supporting CIFs are concentrated to a single ICT TPSP or a small number of such service providers;

i. the transferability of the ICT services supporting CIFs to another ICT TPSP, including as a result of technology specificities;

j. the potential impact of disruptions in the provision of the ICT services supporting CIFs on the continuity of the Financial Entity's activities and on the availability of its services.[31]

31 Art. 1 RTS.

4. GOVERNANCE ARRANGEMENTS

4. GOVERNANCE ARRANGEMENTS

The ultimate responsibility of the management body to manage the Financial Entity's ICT risk is an overarching principle under DORA, which also applies to the use of ICT TPSPs. This responsibility must be further translated by the Financial Entity into the continuous engagement of the management body in the control and monitoring of ICT risk management.

Against this background, the RTS require the management body of a Financial Entity to adopt the TP ICT Policy in writing, and ensure its implementation on an individual, and, as applicable, on a sub-consolidated and consolidated basis (see above). The management body must review the TP ICT Policy at least annually, and update it where necessary.[32] Although risk management and IT security functions may, in practice, be involved in the review process, the responsibility to carry out the review (including deciding on findings, needed policy or implementation changes) should be with the management body. This annual review frequency of the TP ICT Policy is quite intensive for most Financial Entities and will provide for a considerable compliance burden. The ESAs considered the annual cycle appropriate, given the rapid expansion and innovation of ICT service provision to Financial Entities. Nevertheless, in the event of limited changes to the DORA and factual framework, the annual review may be proportional and can thus be (more) swiftly performed.

Changes made to the TP ICT Policy must be implemented in a timely manner and as soon as it is possible within the relevant contractual arrangements. In this context, "timely" means that changes made to the TP ICT Policy must be implemented in a reasonable time period.[33] The ESAs stipulate that it would not be possible to set a single time period for the multitude of different changes that may require implementation, and that the phrase "as soon as possible" has been included to provide some leeway for Financial Entities and competent authorities to take into account situations where a very large number of contracts would have to be updated following the review of the TP ICT Policy. Moreover, the Financial Entity must document the planned timeline for the implementation.

32 Art. 3(1) RTS.

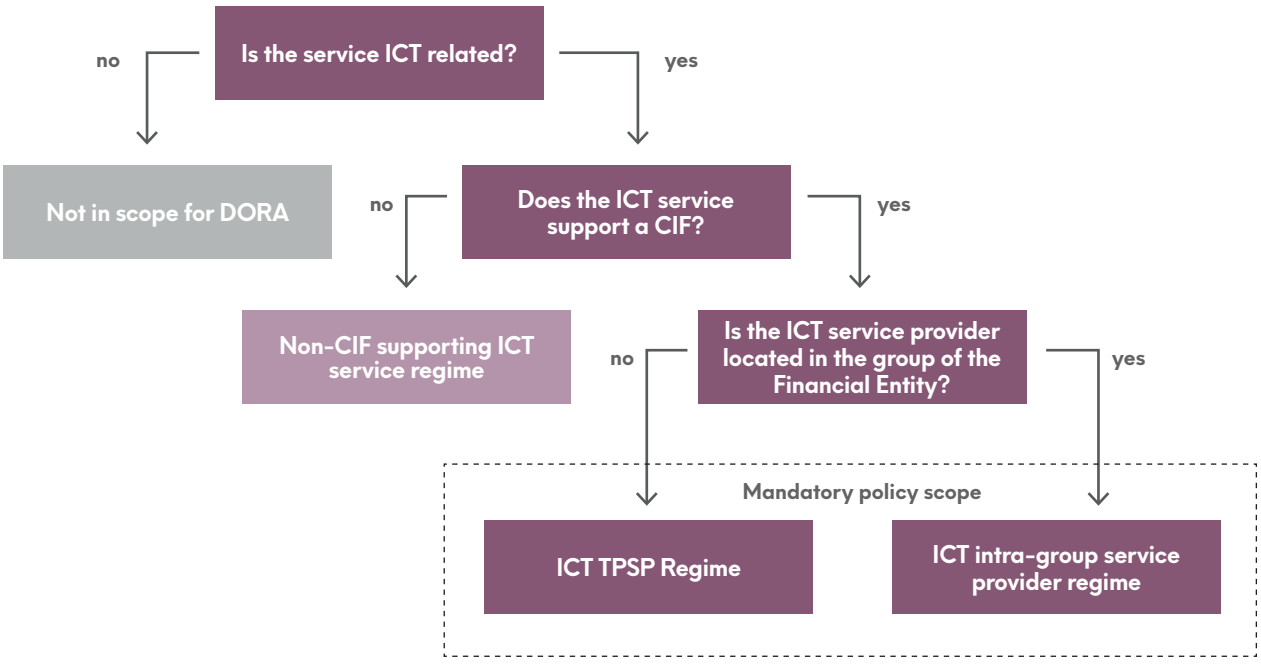
33 Final Report on draft RTS, p. 37.

4.1 Elements of the TP ICT Policy

Below, we cover the concrete elements that must be included in the TP ICT Policy, setting out the legal requirements under the RTS and sharing certain observations regarding the implementation thereof in the TP ICT Policy. We note that in addition to the concrete elements set out in the RTS, the TP ICT Policy should comprise other relevant aspects of DORA not per se related to ICT third-party risk management where relevant and appropriate.[34]

Arguably the most important requirement of the TP ICT Policy involves the mechanism that serves to differentiate between ICT TPSPs providing services that support CIFs and those that do not. We have included a basic flow chart below that could be used at the time of ICT TPSP engagement to determine the applicability of the TP ICT Policy to any ICT relation. We note that the outcome of the assessment is not static, but needs to be reviewed, for instance during the annual review or in light of an alteration in the relationship between the Financial Entity and the ICT TPSP.

Figure 1: DORA TP ICT Policy scope decision tree



34 Art. 8(1) RTS and 1(1)(a) DORA.

The TP ICT Policy must also:

a clearly assign the internal responsibilities for the approval, management, control, and documentation of relevant contractual arrangements and must ensure that appropriate skills, experience and knowledge are maintained within the Financial Entity to effectively oversee the relevant contractual arrangements, including the ICT services provided under these arrangements, i.e., ensure that a proper governance structure is created which ensures that sufficiently skilled (human) resources are available for the prudent management of ICT TPSP risk;

b foresee that the Financial Entity assesses that the ICT TPSP has sufficient resources to ensure that the Financial Entity complies with all its legal and regulatory requirements regarding ICT services supporting CIFs that are provided, i.e. as a part of the due diligence process;

c clearly identify the role or member of senior management[35] responsible for monitoring the relevant contractual arrangements, whereby it defines how this role or member of senior management cooperates with the control functions where it is not part of it and define the reporting lines to the management body, including the nature and frequency of the documents to report, i.e., create a clear division of responsibilities in the governance structure;

d ensure that the relevant contractual arrangements are consistent with the Financial Entity's ICT risk management framework, the information security policy, the business continuity policy and the requirements on incident reporting, i.e., ensure that the contractual terms that are entered into with ICT TPSPs are commensurate to the TP ICT Policy and related DORA documentation and not merely a copy of the DORA contractual requirements;

e require that ICT services supporting CIFs provided by ICT TPSPs are subject to independent review[36] and included in the Financial Entity's audit plan. For the avoidance of doubt, this requirement does not impose a mandatory audit frequency and does not impose to have a separate audit plan for outsourcing and third-party risk management;[37]

35 "Senior management" in this context refers to senior management as it is usually defined by sectoral directives. For example, under Directive 2013/36/EU it means: those natural persons who exercise executive functions within an institution and who are responsible, and accountable to the management body, for the day-to-day management of the institution.

36 Independent review means from the Financial Entity's internal audit or an appointed third party.

37 Final Report on draft RTS, p. 40.

f explicitly specify that the relevant contractual arrangements:

I do not relieve the Financial Entity and its management body of its regulatory obligations and its responsibilities to its clients;

II do not hinder effective supervision of a Financial Entity and shall not contravene any supervisory restrictions on services and activities;

III have provisions in place that ensure that the ICT TPSPs cooperate with the competent authorities; and

IV have provisions in place that ensure that the Financial Entity, its auditors, and competent authorities have effective access to data and premises relating to the use of ICT services supporting CIFs. For the avoidance of doubt, the access right should be limited to the contractual arrangement related to the use of ICT services supporting CIF provided by the ICT TPSP.[38] Physical access to data centres belonging to cloud service providers should also be foreseen.[39]

In respect of the requirement under (f), we note that where an ICT TPSP disagrees to include audit, information and access rights clauses in the relevant contractual arrangement, the Financial Entity should not enter into the contractual arrangement as it would not be able to comply with its regulatory requirements.[40]

38 Final Report on draft RTS, p. 41.
39 Ibid.
40 Ibid.

5.
MAIN PHASES OF THE LIFECYCLE FOR THE USE OF ICT SERVICES

5. MAIN PHASES OF THE LIFECYCLE FOR THE USE OF ICT SERVICES

The TP ICT Policy must cover the entire lifecycle of the business relation with the ICT TPSP, not only the contractual phase. Therefore, it is essential that the TP ICT Policy is drafted in such a manner that it is consulted before a concrete intention to engage into a relation with an ICT TPSP is formed, already becoming applicable in the orientation phase and remaining applicable after termination. For each of these phases in the lifecycle the TP ICT Policy must specify the requirements, including principles, responsibilities and the processes pertaining thereto, covering at least:

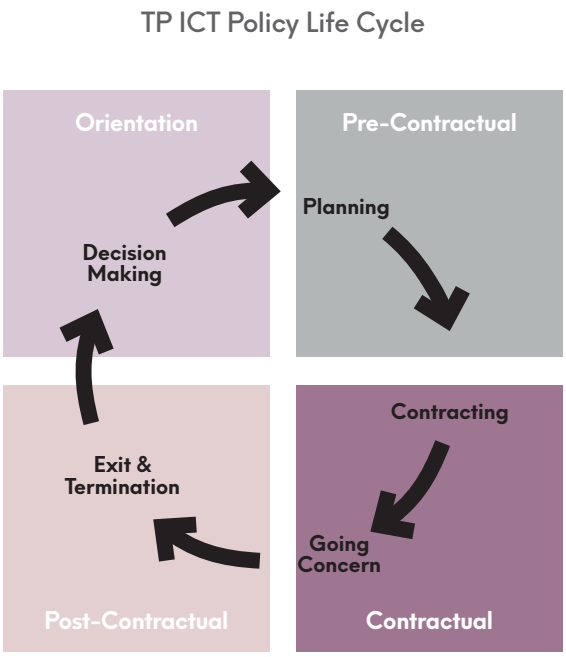
- **a** the responsibilities of the management body, including its involvement, as appropriate, in the decision-making process on the use of ICT services supporting CIFs provided by ICT TPSPs. Regarding the involvement of the management body, it has been clarified that the involvement of the management is foresee "as appropriate" regarding the decision-making process on the use of ICT services supporting CIFs provided by ICT TPSPs. It is therefore not required to involve the management body on a systematic basis;[41]
- **b** the planning of contractual arrangements for the use of ICT services supporting CIFs provided by ICT TPSPs including the risk assessment (as referred to in paragraph 6.1), the due diligence (as referred to in paragraph 6.2) and the approval process of new or material changes to relevant third-party contractual arrangements;
- **c** the involvement of business units[42], internal controls[43] and others relevant units in respect of contractual arrangements for the use of ICT services supporting CIFs provided by ICT TPSPs;
- **d** the implementation, monitoring and management of contractual arrangements for the use of ICT services supporting CIFs including at consolidated and sub consolidated level, where applicable;
- **e** the documentation and record-keeping, taking into account the requirements on the register of information in accordance with Article 28(3) of DORA; and
- **f** the exit strategies and termination processes (as referred to below (art. 10 RTS)).

41 Final Report on draft RTS, p. 44.

42 The involvement of business units refers to the involvement of operational functions.

43 The involvement of internal control units refers to the internal control units as they are generally defined in sectoral directives, i.e., the units that are usually independent from the business they control.

Figure 2:TP ICT Policy life cycle elements



The rationale behind the lifecycle scope of the TP ICT Policy is that the ESAs believe that the coverage of contractual arrangements from the pre-contractual phase to the exit-phase ensures an appropriate, comprehensive and sound risk management framework, covering all relevant aspects surrounding an ICT service, delivering on the harmonising and all-encompassing mandate of DORA.

We note in respect of point (a) that during the orientation phase, i.e., before a concrete ICT service provider is envisaged to be engaged, a Financial Entity needs to ensure that it has a proper governance structure in place. The TP ICT Policy will serve this purpose and should enable the Financial Entity to understand:

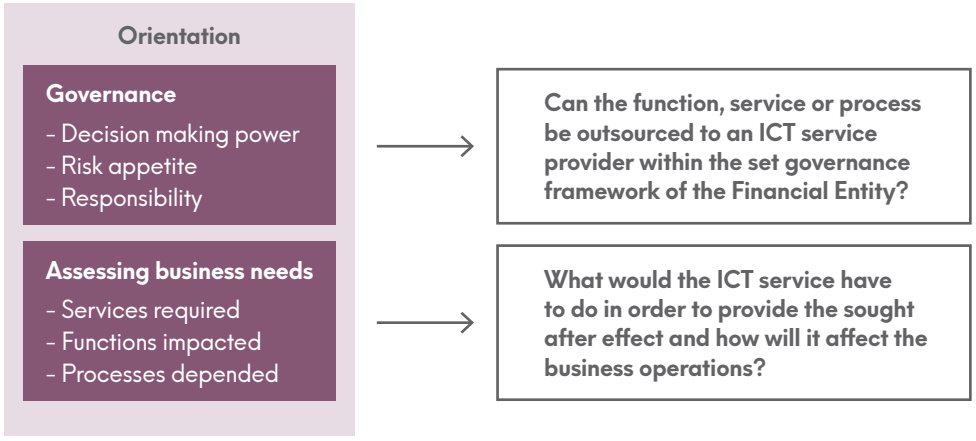
I what it thinks of outsourcing to an ICT service provider, i.e., does it concern a single service, a process or even a whole function? These questions matter for the level of intensity of the TP ICT Policy measures, but also for the cross-application of other policies and procedures available at the Financial Entity, clarity on which will ultimately create a more workable operational system;

II what are the parameters that determine what ICT service can be used and what the control measures of such use need to be;

III who is responsible for the monitoring, engaging and controlling of the ICT services, whereby the ultimate responsibility always resides with the management board;

IV who can take decisions on engaging ICT services and how is it ensured that the organisation as a whole is aware of the ICT service being provided by an external party.

Figure 3: Orientation elements

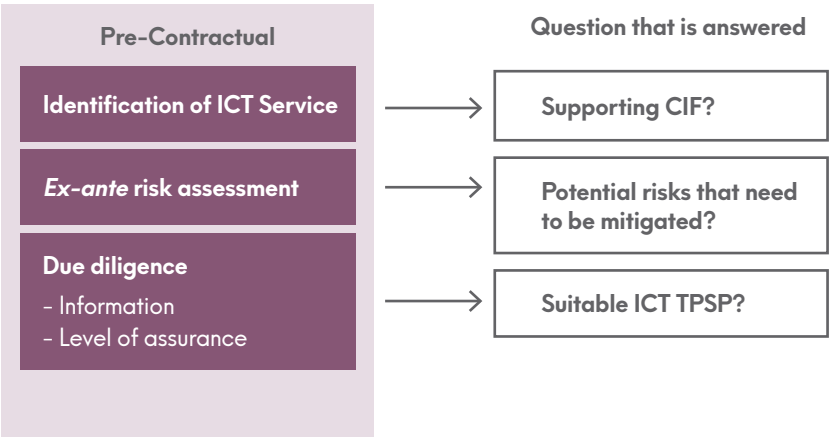


6.
PRE-CONTRACTUAL PROCESS

6. PRE-CONTRACTUAL PROCESS

In this section, we touch on the requirements for the TP ICT Policy for the pre-contractual phase, being that period of time spanning from the decision to *engage an* ICT TPSP until the moment, but not including, the contracting with a *specific* ICT TPSP.

Figure 4: Pre-contractual phase



6.1 *Ex-ante* risk assesment

Pursuant to art. 5 RTS, the TP ICT Policy must include the requirement to define the business needs of the Financial Entity before entering into contractual arrangements on the use of ICT services provided by prospective ICT TPSPs that support CIFs. In addition, the TP ICT Policy must require that, before entering into a contractual arrangement with an ICT TPSP, a risk assessment will be conducted at Financial Entity level, and, where applicable, at consolidated and sub-consolidated level. Based on the output of the risk assessment, a Financial Entity can evaluate what its specific business needs are for the given ICT service relation, aligning the identified risks with the TP ICT Policy. Hence, a single risk assessment on consolidated level is generally not considered sufficient, as the individual subsidiaries need to be able to identify their business needs. What is possible, is a far-reaching alignment of business needs, pursuant also to the consolidated application of the TP ICT Policy, whereby the output of the *ex-ante* risk assessment will be largely equivalent, bar the subjects where the individual TP ICT Policy deviates from the consolidated TP ICT Policy.[44]

44 Final Report on draft RTS, p. 45.

The risk assessment must consider, in particular, the impact of the provision of ICT services supporting CIFs by ICT TPSPs on the Financial Entity and all its risks, including operational risks, legal risks, ICT risks, reputational risks, risks to the protection of confidential or personal data, risks linked to the availability of data, risks linked to where the location of the data is processed and stored and the location of the ICT TPSP as well as ICT concentration risks at entity level.[45] This risk assessment very much resembles the pre-contractual risk assessment as set out in the EBA Guidelines, which requires institutions to assess the potential impact of outsourcing arrangements on their operational risk, to take into account the assessment results when deciding whether the function should be outsourced to a service provider and take appropriate steps to avoid undue additional operational risks before entering into outsourcing arrangements.[46] Similarly, the ESMA Guidelines require the institution to assess all relevant risks that may arise as a result of the cloud outsourcing arrangement, including risks in relation to *inter alia* ICT and information security.[47]

Accordingly, before entering into an arrangement with an ICT TPSP for the use of ICT services supporting CIFs, an *ex-ante* risk assessment should be performed by the Financial Entity as part of its mandatory risk management under DORA. During this phase, the relevant ICT TPSP must provide the Financial Entity with the information necessary for those purposes to ensure that the Financial Entity that would enter into contractual arrangements without making such assessment would not be breaching regulatory requirements. It shall be mandatory for the Financial Entity to ascertain the applicable security standards, where principally these shall have to be the most up-to-date and of the highest quality.

45 In accordance with art. 29 DORA.
46 EBA Guidelines, para. 64.
47 ESMA Guidelines, para. 21.

We note that this *ex-ante* risk assessment is specifically required to be the same for both ICT TPSPs and intragroup service providers. The ESAs are of the opinion that these risks would have to be considered at an individual basis due to potential future events like resolution or sale. Moreover, they believed that the lack of such requirements at intragroup level may lead to a situation where the same standards would not be applied for intragroup service providers, leading to an underestimation of risks related to ICT services.[48] We underline the importance of these arrangements for the Dutch market, as the current derogation for intragroup outsourcing will be removed effective 1 July 2024.[49]

6.2 Due diligence

Under the EBA Guidelines, institutions should, before entering into an outsourcing arrangement and considering the operational risks related to the function to be outsourced, ensure in their selection and assessment process that the service provider is suitable. This means, more specifically with regard to critical and important functions, that Financial Entities must ensure that the service provider has the business reputation, appropriate and sufficient abilities, the expertise, the capacity, the resources, and the organisational structure to perform the function in a reliable and professional manner to meet its obligations over the duration of the contract.[50] Additional factors to be considered when conducting due diligence on a potential service provider include, but are not limited to:

- **a** its business model, nature, scale, complexity, financial situation, ownership and group structure;
- **b** the long-term relationships with service providers that have already been assessed and perform services for the institution;
- **c** whether the service provider is part of the same group;
- **d** whether or not the service provider is supervised by competent authorities.

48 Final Report on draft RTS, p. 23.

49 Art. 32 *Besluit prudentiële regels*, will be removed effective 1 July 2024 in the final effort of the Dutch government to become compliant with the Outsourcing Guidelines.

50 EBA Guidelines, para. 70.

The ESMA Guidelines include similar requirements to evaluate the suitability of a third-party service provider. However, the ESMA Guidelines place additional focus on ICT-related aspects such as the management of information security and in particular the protection of personal, confidential or otherwise sensitive data, and the business continuity and disaster recovery plans.[51]

It appears to us that the due diligence requirements under DORA in this respect are far more comprehensive as they include very specific elements that a Financial Entity should consider and also require specific levels of assurance in respect of the risk management framework of the service provider. In accordance with art. 28(4) DORA, the TP ICT Policy must specify an appropriate and proportionate process for selecting and assessing the prospective ICT TPSP. Such process should take into account whether or not the ICT TPSP is an intragroup ICT service provider, applying a slightly lighter due diligence process to intragroup providers as compared to the thorough assessment of ICT TPSPs. Generally, however, the due diligence process ought to enable the Financial Entity to identify whether the ICT TPSP:

a has the business reputation, sufficient abilities, expertise and adequate financial, human and technical resources, information security standards, appropriate organisational structure, risk management and internal controls and, if applicable, the required authorisation(s) or registration(s) to provide the ICT services supporting the CIF in a reliable and professional manner, the ability to monitor relevant technological developments and identify ICT security leading practices and implement them where appropriate to have an effective and sound digital operational resilience framework;

b The level of certifications based on independent standards (ISO, PCS-DSS, etc.);

c uses or intends to use ICT sub-contractors to perform ICT services supporting CIFs or material parts thereof;

d is located, or processes or stores data in a third country and if this is the case, if this practice elevates the level of operational risks, reputational risks or the risk of being affected by restrictive measures, including embargos and sanctions, that may impact the ability of the ICT TPSP to provide the ICT services or the Financial Entity to receive those ICT services;

51 ESMA Guidelines, para. 22.

e consents to arrangements that ensure that it is effectively possible to conduct audits, including onsite, by the Financial Entity itself, appointed third parties, and competent authorities at the ICT service provider;

f acts in an ethical and socially responsible manner and adheres to human and children's rights, applicable principles on environmental protection, and ensures appropriate working conditions including the prohibition of child labour.

The TP ICT Policy must specify the required level of assurance concerning the effectiveness of ICT TPSPs' risk management framework for the ICT services to be provided by ICT TPSPs to support CIFs, i.e., the level to which the information provided by the ICT TPSP is (independently) verified and supported. In the context of this requirement, the TP ICT Policy shall determine which of the following elements shall be used for obtaining the required level of assurance of the ICT TPSP's service performance:

1) audits or independent assessments performed by the Financial Entity itself or on its behalf;
2) the use by the Financial Entity of independent audit reports made on behalf of the ICT TPSP;
3) the use by the Financial Entity of audit reports of the internal audit function of the ICT TPSP;
4) the use by the Financial Entity of relevant appropriate third-party certifications (e.g., ISO or PCS-DSS);
5) the use by the Financial Entity of other relevant available information or other information provided by the ICT TPSP.

The required level of assurance, and the requisite level of independence of the manner in which it is obtained – i.e., which of the above elements under 1 to 5 is used, needs to be proportional to the ICT service provided. In the event of highly important or risky relations, more than one element must be used to obtain a sufficient level of assurance.

The TP ICT Policy must furthermore require that the due diligence process includes a further (risk) assessment of (i) the mitigating factors for the risks identified in the *ex-ante* risk assessment, (ii) the existing business continuity measures and (iii) including how their functioning within the ICT TPSP is ensured. In view of the fact

that business continuity plans are usually highly confidential and therefore unlikely to be shared for due diligence, even under a non-disclosure agreement, the ESAs have clarified that the requirement is on ensuring the existence of risk mitigation and business continuity measures and how their functioning within the ICT TPSP is ensured, meaning that the actual business continuity plans do not have to be subject of the due diligence.

> In case of intragroup service providers, the fact that the ICT service provider is an intragroup service provider must be considered. As such, the assessment of the above aspects can rely on already established facts by the Financial Entity. However, the Financial Entity must still assess whether the intragroup service provider is suitable to provide the relevant service.

In respect of (b), we note that due diligence to be performed by the Financial Entity concerns in particular the ICT TPSP who is responsible to perform due diligence assessments regarding subcontractors, including when new subcontracts are added. The due diligence assessment should therefore consider the risks and possible changes to risks caused by subcontracting (of a part) of the ICT service by the ICT TPSP and generally the TP ICT Policy shall also apply to subcontracting relations.[52] We note that specific regulatory technical standards in respect of subcontracting have been developed by the ESAs and are currently awaiting adoption by the Commission.[53]

In respect of point (d) we note that the requirement to be able to perform audits seems like a high bar to set for the pre-contractual phase. Although this can surely be the case, the RTS leaves room for leveraging on audits performed by independent third-parties, which the ICT TPSP may already have been subject to regarding the service provided to another Financial Entity. This notwithstanding the audit right of the competent authority or, incidentally, that of the Financial Entity itself. Moreover, the level of assurance could be (partially) reached by leveraging on existing due diligence reports from independent third-parties that have performed a DORA

52 Recital (5) RTS.

53 ESA Consultation Paper on Draft Regulatory Technical Standards to specify the elements which a Financial Entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554.

compliant due diligence process of the ICT TPSP on behalf of other Financial Entities or branch organisations. It shall be up to the responsible Financial Entity to prove that such pre-existing due diligence reports provide a sufficient level of assurance.

In respect of (e), we note that that this requirement seems to be copied from Paragraph 73 from the EBA Guidelines. However, there has been quite some discussion around whether the due diligence should include due diligence on acting in an ethical and socially responsible matter, as these requirements will be contained in more detail in the upcoming Corporate Sustainability Due Diligence Directive, may exceed the legislative mandate for the RTS and does not address DORA resilience aims. The ESAs are however of the opinion that these aspects are still relevant in the case of ICT third-party risk management. That being said, they note that the European Charter of Fundamental Rights already establishes certain values that must be complied with within the EU. Such principles, including the observance of human rights must be complied with also where the Financial Entities rely on service providers and subservice providers, including those located in third countries that are not directly subject to the aforementioned Charter.

6.3 Conflicts of interest

The TP ICT Policy must specify the appropriate measures to identify, prevent and manage actual or potential conflicts of interest arising from the use of ICT TPSPs before entering into relevant contractual arrangements and provide for an ongoing monitoring of conflicts of interest. The requirement to include the management of conflicts of interest in the TP ICT Policy is a further substantiation of DORA, and particularly art. 28(4)(e) DORA which sets out that Financial Entities must identify and assess conflicts of interests that may be caused by contractual arrangements. In that sense, the conflict of interest provision of DORA and the RTS are a supplement to the range of existing conflicts of interest rules applicable to Financial Entities, such as those included under *inter alia* the UCITS Directive, AIFMD and MiFID II.

> Where ICT services are provided by ICT intragroup service providers, the TP ICT Policy must specify that decisions on conditions, including the financial conditions, for the ICT service supporting CIFs are taken objectively.

For comparison, it follows from the EBA Guidelines that institutions should identify, assess, and manage conflicts of interest with regard to their outsourcing arrangement.[54] Where outsourcing creates *material* conflicts of interest, including between entities within the same group, institutions need to take appropriate measures to manage those conflicts of interest.[55] Interestingly, however, the EBA Guidelines stipulate that when functions are provided by a service provider that is part of a group, the conditions, including financial conditions, for the outsourced service should be set at arm's length. A similar phrase was included in the original version of art. 7(2) DORA, however, the wording that the "conditions (...) should be set at arm's length" has been replaced in the final version (by "the decisions on conditions are taken objectively"), following comments from the consultations, including that it would be unclear how the conditions can be specified to be set at arm's length in the TP ICT Policy and questions as to the legal mandate to include such a concept.[56]

We note that the ESMA Guidelines only include a very general requirement for the institution to, before entering a cloud outsourcing arrangement, identify and assess any conflict of interest that the outsourcing may cause.[57]

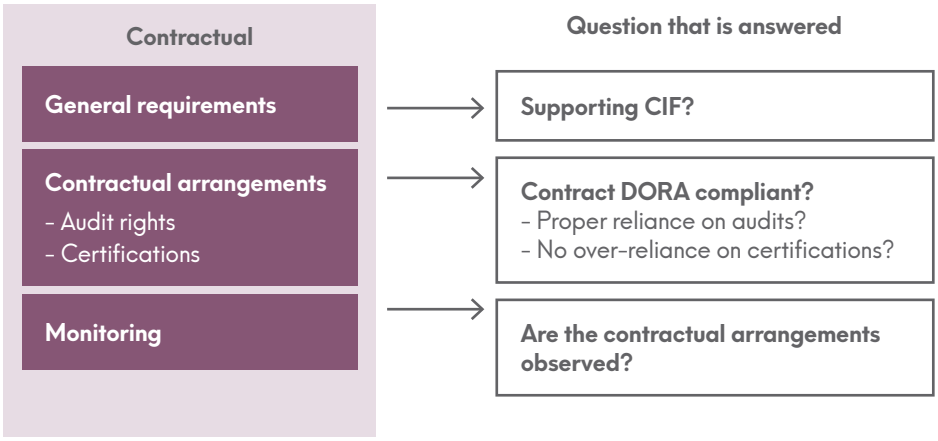
54 EBA Guidelines, para. 45.
55 EBA Guidelines, para. 46.
56 Final Report on draft RTS, p. 48.
57 ESMA Guidelines, para. 19.

7.
CONTRACTUAL PHASE

7. CONTRACTUAL PHASE

In this section, we touch on the requirements during the contractual phase of an ICT service, i.e., the time span from the conclusion of the contract up to, but not including, the termination of the contract. We shall first touch on the requirements in respect of the TP ICT Policy for the contractual safeguards and, second, we will discuss the monitoring obligations and the implementation thereof in the TP ICT Policy.

Figure 5: Contractual phase elements



7.1 Contractual Requirements

7.1.1 Legal requirements

The TP ICT Policy must specify that the relevant contractual arrangement must be in written form and include all elements as set out in art. 30(2) and (3) DORA.[58] Pursuant to Art. 30(1) DORA, the rights and obligations of the Financial Entity and of the ICT TPSP must be clearly allocated and set out in writing. The full contract must include the service level agreements (SLA) and be documented in one (1) written document which needs to be available to the contracting parties on paper, or in a document with another downloadable, durable and accessible format, i.e., PDF. When negotiating contractual arrangements, Financial Entities and ICT TPSPs must consider the use of standard contractual clauses developed by public authorities for specific services.

58 Art. 8(1) RTS.

7.1.2 Elements in contractual arrangements on the use of ICT services

The TP ICT Policy must regulate that the contractual arrangements on the use of ICT services must include at least the contractual arrangements listed in art. 30 DORA, regardless of whether the ICT service provider is provided by an ICT TPSP or an intra-group service provider. DORA, in principle, provides for detailed requirements that may be further refined in standard contractual clauses developed by public authorities, or as developed by industry bodies. We do not discuss the concrete contractual requirements further here as these are beyond the scope of this paper. Nevertheless, we included an overview of the contractual arrangements and a comparison thereof with the Current ESA Outsourcing Guidelines as an Appendix to this paper. We do, however, pay specific attention to two aspects in the contractual phase below:

I the contractual arrangements in respect of audit rights; and

II the reliance on third-party certificates or audit reports for the purposes of such contractual audit rights.

7.1.3 Audit arrangements

Under the EBA Guidelines, institutions must ensure within the written outsourcing arrangement that the internal audit function – insofar established – is able to review the outsourced function using a risk-based approach. With regard to the outsourcing of CIFs, institutions must ensure within the written outsourcing agreement that the service provider grants them and their competent authorities, including resolution authorities, and any other person appointed by them or the competent authorities, the following audit rights:

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 service provider's external auditors; and

II unrestricted rights of inspection and auditing related to the outsourcing arrangement to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.

The ESMA Guidelines include a less detailed requirement, setting out that the firm should ensure that the outsourcing written agreement does not limit the firm's and competent authority's effective exercise of the access and audit rights and oversight options on the service provider.[59]

Although it appears that certain market parties fear that Financial Entities have low bargaining power regarding many of the more demanding contractual requirements (e.g., demanding of additional certification or conducting the TLPT), the ESAs emphasised that almost the entire financial sector is required to have those clauses in place, so that ICT TPSPs must agree with the requirements under DORA as otherwise Financial Entities cannot enter into a contractual arrangement with them. Under DORA, these mandatory (audit) rights have been included in a Regulation, lending authority to Financial Entities that attempt to include such rights in their contracts with ICT TPSPs. This taken together with the critical ICT TPSP regime, which should put the largest and most important TPSPs such as Amazon and Microsoft under oversight of the ESAs, and the standardised terms issued by public authorities, should provide for a much easier process of arranging audit rights.[60] Nevertheless, Financial Entities will continue to experience difficulty in arranging the appropriate audit rights, especially if ICT TPSPs from outside the EU are engaged.

However, it is also common knowledge that certain ICT TPSPs, especially the large and well-established ones, historically tend to have contractual arrangements in place accommodating for these specific audit rights, as they are aware of the regulatory expectations and obligations of their Financial Entity clients. In such cases, it will be less problematic to ensure acceptance of these specific contractual provisions by such ICT TPSPs, and the Financial Entity may rely on the existing or standardised terms and conditions of the ICT TPSP, provided that they are in line with the RTS and DORA requirements. The TP ICT Policy should specify how the Financial Entity verifies the adequacy and effectiveness of the contractual audit rights, and how it assesses the quality and reliability of the audits and ICT testing conducted by the ICT TPSP or a third party on its behalf.

59 Para. 34 of the ESMA Guidelines.
60 Final Report on draft RTS, p. 49.

Against that background, the RTS require that the TP ICT Policy specifies that the contractual arrangements with ICT TPSPs include information access, inspection, audit, and ICT testing rights.[61] These rights, as also described in art. 30 DORA, ought to be described in the TP ICT Policy as to what purpose they serve, how they might take form and when what type of iteration of the audit right is applied. For such implementation of the audit right the Financial Entity has a range of methods to choose from, which have to be embedded within the TP ICT Policy. These could be, without prejudice to the final responsibility of the Financial Entity, the following:

- **a** its own internal audit or an appointed third party;
- **b** where appropriate, pooled audits and pooled ICT testing, including TLPT, organised jointly with other contracting Financial Entities or firms that use ICT services of the same ICT TPSP, that are performed by them and these contracting Financial Entities or firms or by a third party appointed by them;
- **c** where appropriate, third-party certifications;
- **d** where appropriate, third-party or internal audit reports made available by the ICT TPSP.

As such, the use of the Financial Entity's internal audit or an appointed third party is mandatory, and pooled audits, third-party certifications and reports may be used where appropriate in course of the exercise of the contractual audit right.[62] This appears broadly in line with requirements under para. 91 under the EBA Guidelines and para. 37 of the ESMA Guidelines, which stipulate that institutions may use pooled audits organised jointly with other clients of the same service provider, and third-party certifications and third-party or internal audit reports made available by the service provider.

61 Art. 8(2) RTS.

62 Final Report on draft RTS, p. 49.

7.1.4 Third-party certifications and audit reports

One of the key elements of the TP ICT Policy is to establish a view on the security standards that must be met by the ICT TPSPs and how these standards will be verified by the Financial Entity. However, in practice, there may be a tendency for the Financial Entity to rely on the self-assessment or certification of the ICT TPSPs regarding their compliance with widely recognised security standards, such as ISO 27001 or PCI DSS. This may reduce the burden for the Financial Entity to conduct its own due diligence or audit of the ICT TPSPs, but it also implies a degree of trust and acceptance of the risk that the ICT TPSPs may not fully adhere to the security standards or that the standards may not be sufficient to address the specific risks faced by the Financial Entity. In respect of the third-party certifications and reports under (c) and (d) respectively, we specifically note that these may not solely be relied upon over time, i.e., the Financial Entity may not only request certifications and third-party audit reports for the fulfilment of its audit of the performance of the ICT TPSP. The use of such third-party audit affidavits is subject to certain edge conditions, which need to be embedded within the TP ICT Policy, requiring that the Financial Entity:[63]

- **a** is satisfied[64] with the audit plan of the ICT TPSP for the relevant contractual arrangements;
- **b** ensures that the scope of the certifications or audit reports cover the systems and key controls identified by the Financial Entity and the compliance with relevant regulatory requirements;
- **c** thoroughly assesses the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete;
- **d** ensures that key systems and controls are covered in future versions of the certification or audit report;[65]
- **e** is satisfied with the aptitude of the certifying or auditing party;
- **f** is satisfied that the certifications are issued, and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;

63 Art. 8(3) RTS.

64 "Satisfied" means that the Financial Entity should determine that it is able to rely on the results of its audit plan to accurately reflect the risk level of the arrangement.

65 The ESAs note that audit reports and certifications need to ensure transparency as otherwise Financial Entities are unable to value the audit findings or certification significance and as a result would be unable to contract with the ICT TPSP.

g has the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls, whereby the number and frequency of such requests for scope modification must be reasonable and legitimate from a risk management perspective; and

h retains the contractual right to perform individual and pooled audits at its discretion with regard to the relevant contractual arrangements and execute them in line with the contracted frequency.

This requirement is an almost one-on-one copy of the requirements under para. 93 of the EBA Guidelines and para. 39 of the ESMA Guidelines. As such, third-party certifications can be used by the Financial Entity for purposes of its inspection, audit and ICT testing, however, it should not be the only measure taken to monitor the ICT service related to the CIF. Where relied upon by the Financial Entity, the use of third-party certifications and audit reports shall at least have to be clearly regulated in the TP ICT Policy, setting out the appropriate governance thereof in light of the edge conditions mentioned above. Ultimately, the final responsibility for the audit lies with the Financial Entity where a high-level of supervisory assurance must be ensured for the correct functioning of the financial markets.[66]

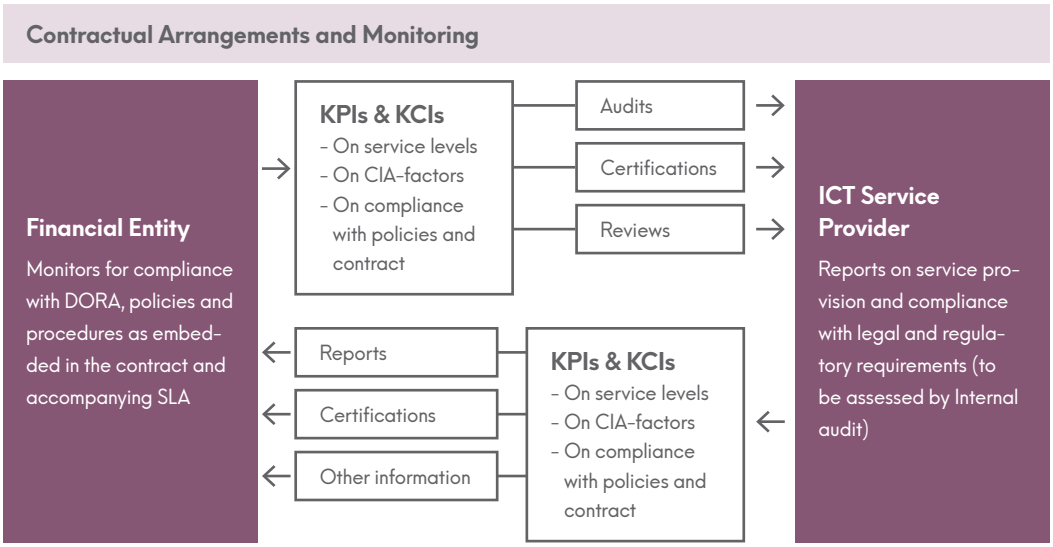
Lastly, the TP ICT Policy needs to ensure that material changes to the contractual arrangements are to be formalised in a written document, e.g., an amendment agreement or appendix, which shall have to be dated and signed by all parties involved in the ICT service relation. For example, if the group entity has concluded a contract that also covers service provision to the subsidiaries, theoretically the subsidiaries should also be signatories to the amendment agreement.

66 Final Report on draft RTS, p. 49.

7.2 Monitoring of the contractual arrangements

Under the EBA Guidelines, institutions must monitor, on an ongoing basis, the performance of the service providers with regard to all outsourcing arrangements on a risk-based approach and with the main focus on the outsourcing of CIFs, including that the availability, integrity and security of data and information is ensured. They must ensure that the outsourcing arrangements meet appropriate performance and quality standards in line with their policies by (i) ensuring that they receive appropriate reports from service providers, (ii) evaluating the performance of service providers using tools such as key performance indicators, key control indicators, service delivery reports, self-certification and independent reviews, and (iii) reviewing all other relevant information received from the service provider, including reports on business continuity measures and testing.

Figure 6: Overview of monitoring phase



Under DORA, the TP ICT Policy must ensure that the relevant contractual arrangements specify the measures and key performance indicators ("**KPIs**") to monitor, on an ongoing basis, to assess the performance of ICT TPSPs, including measures to monitor compliance with requirements regarding the confidentiality, availability, integrity and authenticity of data and information, and the compliance of the ICT TPSPs with the Financial Entity's relevant policies and procedures. The TP ICT Policy should also specify measures that apply when agreed service levels

are not met, including, where appropriate, contractual penalties.[67] In respect of the requirement to monitor the compliance of the ICT TPSPs with the Financial Entity's policy framework, we note that this requirement is addressed to Financial Entities, and that the measures to monitor compliance entails all measures contractually agreed in addition to the ones required by DORA.[68]

The TP ICT Policy must also prescribe how the Financial Entity will assess that the ICT TPSPs (or intra-group provider) used for the ICT services supporting CIFs meet appropriate performance and quality standards in line with the contractual arrangement and the Financial Entity's own policies by ensuring that:[69]

- **a** the ICT TPSPs address appropriate reports on their activities and services provided to the Financial Entity, including periodic reports, incidents reports, service delivery reports, reports on ICT security and on business continuity measures and testing;
- **b** the performance of ICT TPSPs is assessed with KPIs, key control indicators ("**KCIs**"), audits, self-certifications and independent reviews in line with the Financial Entity's ICT risk management framework;
- **c** other relevant information[70] is received from the ICT TPSP;
- **d** the Financial Entity is notified, where appropriate, of ICT-related incidents and operational or security payment related incidents, in accordance with its ICT incident policy pursuant to DORA;[71]
- **e** an independent review and compliance audits with legal and regulatory requirements and policies are performed.

67 Art. 9(1) RTS.

68 Final Report on draft RTS, p. 52; It does not mean that Financial Entities are prohibited from entering into arrangements with ICT providers which offer standard contracts. However, independent of the character of the contract, the Financial Entity has to be aware of the risks and assess whether the contractual clauses are in line with their own relevant policies and procedures and the requirements under DORA.

69 Art. 9(2) RTS.

70 Other relevant information may be any relevant document in the context of performance and quality standards set out in art. 9(2) RTS.

71 For the avoidance of doubt, the requirement is for Financial Entities to ensure that they are informed of incidents.

The "period reports" as referred to under (a) mean reports that are regularly produced, usually with a monthly, quarterly, biannually or annual period. The content of such reports is expected to cover at least the volume of activity and quality of service for the referred period as well as any contractually agreed piece of information. In any case, the Financial Entity shall have to clarify in the TP ICT Policy the types of reporting it expects with general corresponding timeframes and how it will anchor these in the contractual relation.

The KPIs and KCIs referred to under (b) are of paramount importance to embed into the governance of the TP ICT Policy, as it needs to be crystal clear for the Financial Entity who is responsible for the monitoring, what is being monitored and when corrective action needs to be taken. The concrete KPIs and KCIs can be set on an case-by-case basis, however, the general categories of KPIs and KCIs required by the Financial Entity can and must already be set in the TP ICT Policy. This will also aid the Financial Entity in standardising the control environment of each and every ICT service relation.

The "independent review" as referred to under (e) is to be performed by the ICT TPSP's internal audit function (meaning that the scope of this article is different from that of art. 6(3) RTS which focuses on the use of audits within the due diligence process – see paragraph 6.2 above), if established; otherwise it has to be performed by an appointed third party (reference is also made to the requirement under art. 8(2)(a) RTS).

The TP ICT Policy must prescribe that the outcome of the monitoring should be documented and its results used to update the Financial Entity's risk assessment of the ICT service provider.[72] Such update can take place in the yearly review cycle, or in the case of event/incident-driven updates on a more frequent basis. The TP ICT Policy must, furthermore, define the appropriate measures that the Financial Entity shall adopt if it identifies shortcomings of the ICT service provider, i.e., in the case the KPIs or KCIs are breached. This included ICT-related incidents and operational or security payment related incidents, in the provision of the ICT services supporting CIFs or the compliance with contractual arrangements or legal requirements. Moreover, the TP ICT Policy has to detail how the implementation of such measures shall be monitored to ensure that they are effectively complied with by the ICT service provider within the designated timeframe, taking into account the *materiality* of the shortcomings.[73]

72 Art. 9(3) RTS refers to art. 6 RTS (i.e., the due diligence requirement as set out in paragraph 6.2). Based on the context, and the text of the consultated version of the RTS, we assume that this is an unintentional error.

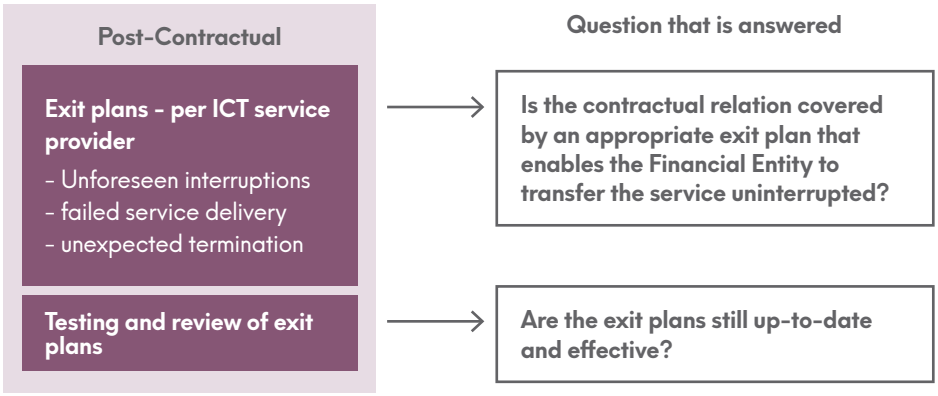
73 Art. 9(4) RTS.

8. EXIT AND TERMINATION OF CONTRACTUAL ARRANGEMENTS

8. EXIT AND TERMINATION OF CONTRACTUAL ARRANGEMENTS

Similar as under the Current ESA Outsourcing Guidelines, the TP ICT Policy must include requirements for a documented exit plan for each *contractual arrangement* on ICT services supporting CIFs provided by an ICT service provider. In other words, in some scenarios it may be possible, especially towards the same ICT TPSP, for exit plans related to a change of the ICT TPSP to be drawn up together, i.e. not requiring to draw up separate exit plans per ICT service but rather per ICT service provider (insofar possible).[74] Exit planning, however, must be clearly separated from business continuity planning. Exit planning always ends with an *exit* whereas business continuity does not necessarily have to end with an exit from the ICT service relationship.

Figure 7: Post-contractual elements



The exit plans must be subject to a periodic review and testing procedure that align the exit plan with realistic, feasible, and plausible scenarios and reasonable assumptions and set out a planned implementation schedule compatible with the exit and termination terms established in the contractual arrangements with the respective ICT service provider. Thus, whilst the TP ICT Policy itself does not necessarily contain the exit plans, it must set out to what conditions they need to

74 Final Report on draft RTS, p. 54.

adhere, when and how they are to be reviewed as well as the process for the testing of the plans. Such exit plan governance should ensure that the exit plans take into account:

- **a** unforeseen and persistent service interruptions;
- **b** inappropriate or failed service delivery;
- **c** the unexpected termination of a relevant contractual arrangement.[75]

The Financial Entity must ensure, by means of the TP ICT Policy, that the exit plan is realistic, feasible, based on plausible scenarios and reasonable assumptions and must have a planned implementation schedule compatible with the exit and termination terms established in the relevant contractual arrangements.[76] It shall be important to adequately clarify the timelines for the exit plans in the TP ICT Policy in order to ensure that such plans adhere to the *exit strategy*, which itself can be described in the TP ICT Policy.

> It should be noted that, whilst the principle of proportionality should apply, these requirements expressly do not differentiate between intragroup and outside group ICT service providers. In this context it may be relevant, for example, to take resolution scenarios into account as they might change the group structure as a result of which an intragroup ICT service provider may afterwards no longer be part of the group of the Financial Entity relying on its ICT services.[77]

Additionally, we recommend Financial Entities to specifically consider any cloud services they may rely on from non-EU service providers (e.g., Amazon, Google, Apple). Non-EU ICT TPSPs providing ICT services supporting CIFs to Financial Entities are in the scope of DORA and Financial Entities relying on their services must ensure that the relevant requirements under DORA are applied.

75 Art. 10 RTS.
76 Ibid.
77 Final Report on draft RTS, p. 56.

9. CONCLUSIONS AND RECOMMENDATIONS

9. CONCLUSIONS AND RECOMMENDATIONS

9.1 Conclusions

DORA seeks to govern the prevention and management of ICT risks by Financial Entities. These risks arise from ICT services provided by ICT TPSPs. DORA impacts all contractual relationships a Financial Entity has with its ICT service providers, irrespective of whether such a contractual relationship qualifies as outsourcing or whether such relationship concerns a CIF. DORA also covers all intra-group ICT arrangements.

Current EU and national legislation already mandate various categories of Financial Entities, including banks, payment institutions, insurers, pension funds, fund managers, and investment firms, to incorporate specific minimum contractual provisions in their material outsourcing agreements, including those related to ICT. It is therefore crucial for such institutions to understand that the requirements in respect of contractual arrangements on the use of ICT services as outlined in DORA are not mere supplements or improvements to existing rules.

The discrepancy generally arises for two main reasons. Firstly, DORA's scope extends beyond existing sectoral outsourcing requirements, such as the Current ESA Outsourcing Guidelines. These guidelines typically apply solely to outsourcing arrangements, possibly restricted to critical or important ones. In contrast, DORA's mandates encompass all ICT contracts, regardless of their outsourcing classification or if they involve generic ICT services provision. Secondly, while there may be some overlap in mandatory contractual requirements between DORA and existing legislation, DORA introduces additional requirements not covered by prior laws. Moreover, even when overlap exists, DORA often specifies more detailed or stringent obligations than its sectoral counterparts. A crucial aspect to note is the comprehensive contractual provisions governing subcontracting by ICT TPSPs.

To clarify, existing legislation only addresses a fraction of a Financial Entity's ICT contract portfolio. Contracts not meeting the outsourcing criteria typically fall outside the scope of existing laws. Even if a Financial Entity has fully implemented the Current ESA Outsourcing Guidelines, only certain DORA requirements will be fulfilled. Additionally, existing ICT outsourcing agreements may lack mandatory clauses stipulated by DORA. Financial Entities not previously subject to the Current ESA Outsourcing Guidelines will need to rectify their entire ICT contract portfolio to comply with DORA.

9.2 Recommendations

To ensure compliance with the extensive Policy requirements, we recommend Financial Entities to consider, *inter alia,* taking the following steps:

- **a** To ensure compliance with the extensive Policy requirements, we suggest that Financial Entities, as a first step, conduct a gap analysis of their current policy framework with the purpose of getting a view on the extent to which their current policy framework aligns with the Policy requirements under DORA;
- **b** Taking into account the results of the gap analysis, we suggest Financial Entities to determine whether to draft a new Policy or incorporate the Policy requirements into their current policy framework. In this regard, we suggest Financial Entities to also take into account the group application requirements, i.e., can the Financial Entity rely on a group-wide Policy (or should a group-wide Policy be drafted?);
- **c** Consequently, we suggest Financial Entities to identify which ICT services are provided to them by third parties (including intra-group entities). As this gives Financial Entities a view on the impact of the ICT third-party risk management requirements, in our view, this is a good starting point to incorporate the Policy requirements in, either a new Policy or into their current policy framework;
- **d** As a next step, we suggest drafting the new Policy (or incorporate the Policy requirements into their current policy framework), especially taking into account into account how the Financial Entity believes compliance with the requirements can be best achieved from an operational perspective; and
- **e** To ensure existing contractual arrangements are compliant with DORA, we recommend using a "DORA compliant" regulatory addendum, which includes all mandatory clauses. As the requirements for critical or important contractual arrangements are more stringent than those for "regular" contractual arrangements, we recommend drafting a "light" "DORA compliant" addendum for the regular arrangements. We suggest to always involve the legal department when drafting the "DORA compliant" addendum, and to consider having an external legal advisor or law firm review the addendum.

Appendix – Contractual Arrangements

Contractual arrangements on the use of ICT services must include at least the following elements:

a a clear and complete description of all functions and ICT services to be provided by the ICT TPSP, indicating whether subcontracting of an ICT service supporting a CIF, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting;

b the locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT TPSP to notify the Financial Entity in advance if it envisages changing such locations;

c provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data;

d provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the Financial Entity in the event of the insolvency, resolution or discontinuation of the business operations of the ICT TPSP, or in the event of the termination of the contractual arrangements;

e service level descriptions, including updates and revisions thereof;

f the obligation of the ICT TPSP to provide assistance to the Financial Entity at no additional cost, or at a cost that is determined *ex-ante*, when an ICT incident that is related to the ICT service provided to the Financial Entity occurs;

g the obligation of the ICT TPSP to fully cooperate with the competent authorities and the resolution authorities of the Financial Entity, including persons appointed by them;

h termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities;

i the conditions for the participation of ICT TPSPs in the Financial Entities' ICT security awareness programmes and digital operational resilience training.

Several of these elements appear to stem from the Current ESA Outsourcing Guidelines, more specifically:

- element (a) resembles:
  - para. 75 under a of the EBA Guidelines, requiring the outsourcing agreement to set out a clear description of the outsourced function to be provided;
  - para. 28 under a of the ESMA Guidelines, requiring the agreement to include a clear description of the outsourced function;
- element (b) resembles:
  - para. 75 under f of the EBA Guidelines, requiring the outsourcing agreement must set out the location(s) (i.e. regions or countries) where the critical or important function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the institution if the service provider proposes to change the location(s);
  - para. 28 under f of the ESMA Guidelines, requiring the agreement to include the location(s) (namely regions or countries) where the outsourced function will be provided and where data will be processed and stored, and the conditions to be met, including a requirement to notify the firm if the service provider proposes to change the location(s);
- element (c) resembles:
  - para 75 under g of the EBA Guidelines, which stipulates that the outsourcing agreement must set out, where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data;
  - para. 28 under g of the ESMA Guidelines, requiring the agreement to include provisions regarding information security and protection of personal data;
- element (d) resembles:
  - para. 75 under m of the EBA Guidelines, which stipulates that the outsourcing agreement must set out provisions that ensure that the data that are owned by the institution can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider;
- element (e) is a basic version of:
  - para. 75 under i of the EBA Guidelines and para. 28 under i of the ESMA Guidelines, requiring that the agreement includes

the agreed service levels, which should include, quantitative and qualitative performance targets in order to allow for timely monitoring so that appropriate corrective actions can be taken without undue delay if agreed service levels are not met;

- element (g) resembles:
  - para. 75 under n of the EBA Guidelines, which stipulates that the outsourcing agreement must set out the obligation of the service provider to cooperate with the competent authorities and resolution authorities of the institution, including other persons appointed by them;
  - para. 28 under
- element (h) resembles:
  - para. 75 under q of the EBA Guidelines, which stipulates that the outsourcing agreement must set out termination rights as set out in Section 13.4 of the EBA Guidelines.

Element (f) and (i) appear "DORA-specific" elements that do not specifically originate from the Current ESA Outsourcing Guidelines.

Additional elements in the event of ICT services supporting CIFs

Contractual arrangements on the use of ICT services supporting CIFs must include, in addition to the elements referred above, at least the following:

a full service level descriptions, including updates and revisions thereof with precise quantitative and qualitative performance targets within the agreed service levels to allow effective monitoring by the Financial Entity of ICT services and enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met;

b notice periods and reporting obligations of the ICT TPSP to the Financial Entity, including notification of any development that might have a material impact on the ICT TPSP's ability to effectively provide the ICT services supporting CIFs in line with agreed service levels;

c requirements for the ICT TPSP to implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide an appropriate level of security for the provision of services by the Financial Entity in line with its regulatory framework;

d the obligation of the ICT TPSP to participate and fully cooperate in the Financial Entity's TLPT;

e the right to monitor, on an ongoing basis, the ICT TPSP's performance, which entails the following:

I unrestricted rights of access, inspection and audit by the Financial Entity, or an appointed third party, and by the competent authority, and the right to take copies of relevant documentation on-site if they are critical to the operations of the ICT TPSP, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;

II the right to agree on alternative assurance levels if other clients' rights are affected;

III the obligation of the ICT TPSP to fully cooperate during the onsite inspections and audits performed by the competent authorities, the lead overseer, Financial Entity or an appointed third party; and

IV the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits;

f exit strategies, in particular the establishment of a mandatory adequate transition period:

I during which the ICT TPSP will continue providing the respective functions, or ICT services, with a view to reducing the risk of disruption at the Financial Entity or to ensure its effective resolution and restructuring;

II allowing the Financial Entity to migrate to another ICT TPSP or change to in-house solutions consistent with the complexity of the service provided.

Several of these elements appear to stem from the Current ESA Outsourcing Guidelines, more specifically:

- element (a) resembles:
  - para. 75 under i of the EBA Guidelines and para. 28 under i of the ESMA Guidelines, requiring that the agreement includes the agreed service levels, which should include, quantitative and qualitative performance targets in order to allow for timely monitoring so that appropriate corrective actions can be taken without undue delay if agreed service levels are not met;
- element (c) includes elements of:
  - para. 75 under l of the EBA Guidelines, requiring that the outsourcing agreement sets out the requirements to implement and test business contingency plans;
  - para. 28 under m of the ESMA Guidelines, requiring that the agreement includes the requirements for the service provider to implement and test business continuity and disaster recovery plans;
- element (e) appears to be an extended version of:
  - para. 75 under p of the EBA Guidelines, requiring that the outsourcing agreement includes the unrestricted right of institutions, and competent authorities to inspect and audit the service provider with regard to, in particular, the critical or important outsourced function;
  - para. 28 under n of the ESMA Guidelines, requiring that the agreement includes the requirement for the CSP to grant the firm, its competent authorities and any other person appointed by the firm or the competent authorities the right to access ('access rights') and to inspect ('audit rights') the relevant information, premises, systems and devices of the CSP to the extent necessary to monitor the CSP's performance under the cloud outsourcing arrangement and its compliance with the applicable regulatory and contractual requirements.

As such, elements (b), (d), (e) and (f) appear "DORA-specific" elements that do not specifically originate from the Current ESA Outsourcing Guidelines.

However, it should be noted that in the financial sector, prevailing practices and standards may already cover some of the elements required by DORA, especially if the ICT services are large-volume or complex. For instance, reporting obligations of the ICT TPSPs are often part of the contractual arrangements and the project governance, ensuring regular and transparent communication between the parties. As such, it will be important to assess the existing governance arrangements and contracts as to whether or not they comply with the DORA requirements in practice, and identify any gaps or areas for improvement.

The TP ICT Policy must also ensure that material changes to these arrangements are formalised in a written document, dated, and signed by all parties and specify the renewal process for contractual arrangements.[78] Accordingly, the contract or agreement with the ICT TPSP must be signed[79], meaning that the contract should be traceable, either in physical or digital form.

****

78 Art. 8(4) RTS.

79 A digital signature is also allowed in view of the recognition of digital signature processes under Regulation EU No 910/2014.