Best Practice Guidance

DORA Contract Compliance

Gorrissen Federspiel

Contents

*The Digital Operational Resilience Regulation, Regulation (EU) 2022/2554 ("**DORA**") requires that twenty-one different types of financial entities covered by the Regulation shall contract with ICT service providers in a manner that complies with detailed contractual requirements. As described in the recitals of DORA, these contractual requirements are intended to provide certain minimum safeguards to strengthen financial entities' ability to effectively monitor all ICT risk emerging at the level of third-party service providers.*

This best practice guidance explains how financial entities can go about establishing contracting compliance.

Executive summary

This guide serves as a tool for financial entities to ensure their ICT service contracts meet the new, stringent requirements set forth by DORA, supplementing existing regulations like the EBA Outsourcing Guidelines and EIOPA Cloud Outsourcing Guidelines.

Key takeaways include:

- DORA applies to all ongoing ICT service contracts, expanding the scope beyond the scope of the EBA Outsourcing Guidelines.
- Financial entities must reassess contracts previously not considered critical or important under EBA Outsourcing Guidelines, as DORA's scope is broader.
- DORA's requirements are more detailed and prescriptive, necessitating updates to contracts to ensure compliance.
- The guidance outlines direct and gives examples of indirect contracting requirements, with indirect requirements also being necessary for financial entities to fulfil their regulatory obligations.
- Strategies for updating existing contracts and drafting new ones are provided.

With a compliance deadline of 17 January 2025, financial entities must act promptly to renegotiate existing contracts and ensure new contracts are DORA-compliant.

This guidance concludes with an annex comparing DORA's direct contracting requirements with the EBA Outsourcing Guidelines, pinpointing the gaps on direct contracting requirements that contracts must address to achieve full DORA compliance. We later shortly issue a similar gap analysis between the EIOPA Cloud Outsourcing Guidelines and DORA.

The existing and past legal requirements to contracting

Introduction

In the recent past, credit institutions, such as banks, have complied with the EBA Guidelines on outsourcing arrangements (the "**EBA Outsourcing Guidelines**") as implemented under Danish law by Executive Order 973 of 22 June 2022 (the "**DEO**") when contracting for outsourced services.

In Denmark, insurance companies have been separated in two groups. Group-1 insurance companies have complied with the broader regulation under article 274 of the Solvency II Delegated Regulation (the "**Solvency II**") and in case of cloud services also the EIOPA Guidelines on outsourcing to cloud service providers of 2021 (the "**EIOPA Cloud Outsourcing Guidelines**")[1]. ATP, Lønmodtagernes Dyrtidsfond and Group-2 insurance companies have complied with Executive order 723 of 28 May 2022 (and not Solvency II as such) and the EIOPA Cloud Outsourcing Guidelines.

DORA does not replace that existing regulation, rather it is complimentary (DORA recital no. 29). This also means that all aspects of the various legislative requirements across multiple types of regulations must be complied with. DORA applies to all contracts on "ICT services" "provided on an ongoing basis" and not only to "outsourcing arrangements" as is the case in respect of the EBA Outsourcing Guidelines. For practical purposes, DORA will apply to all contracts that are within scope of the EBA Outsourcing Guidelines, except potentially BPO outsourcing contracts depending on whether the main component is ICT or relies primarily on ICT (although this not specifically addressed in DORA).

> ***Preamble of DORA, recital no. 69:***
> *"Even though Union financial services law contains certain general rules on outsourcing, monitoring of the contractual dimension is not fully anchored into Union law. In the absence of clear and bespoke Union standards applying to the contractual arrangements*

1 EIOPA Cloud Outsourcing Guidelines apply to all cloud outsourcing arrangements entered into or amended on or after 1 January 2021. "Cloud services" is defined as *"services provided using cloud computing, that is, a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".*

> *concluded with ICT third-party service providers, the external source of ICT risk is not comprehensively addressed. Consequently, it is necessary to set out certain key principles to guide financial entities' management of ICT third-party risk, which are of particular importance when financial entities resort to ICT third-party service providers to support their critical or important functions. Those principles should be accompanied by a set of core contractual rights in relation to several elements in the performance and termination of contractual arrangements with a view to providing certain minimum safeguards in order to strengthen financial entities' ability to effectively monitor all ICT risk emerging at the level of third-party service providers. Those principles are* ***complementary*** *to the sectoral law applicable to outsourcing."*

Lessons learned from previous compliance projects

The financial sector has spent significant resources in upgrading existing contracts with providers of relevant outsourcing services to become compliant with GDPR and contracting requirements and it is with a certain reluctance that a new round of compliance projects must now be initiated.

As a learning from compliance projects related to e.g. EBA Outsourcing Guidelines, many financial entities have found that negotiation or renegotiation contracts for these types of services were difficult at times and not without concessions. In the recitals of DORA, EU recognises the difficulties that financial entities have encountered and mentions specific rights such as securing sufficient access or audit rights and securing sufficient safeguards allowing for the fully-fledged monitoring of subcontract processes. In line with many financial entities experiences, EU recognises that ICT services providers often provide standardised services to different types of clients and such contractual arrangements do not always cater adequately for the individual or specific needs of financial industry actors (DORA recital no. 28). Although DORA entails yet another compliance project, one would assume that service providers servicing the financial services industry have adapted somewhat to the fact that requirements have only increased and will likely continue to do so going forward.

The key question that we are attempting to address is what the gap is between past legal contracting requirements and DORA requirements and which strategies to apply when conducting a DORA contracting compliance project. Put in another manner, to which extent can financial entities rely on contracts having been made "EBA-compliant" or does DORA contract compliance require a greenfield approach? In this best practice guidance, we will provide both high level considerations and input to the detailed analysis of concrete requirements. This is intended to support financial entities in designing efficient strategies on the execution of a DORA contract compliance project.

Briefly on DORA

DORA is a binding EU legislative act that becomes immediately enforceable in all member states. DORA will take effect as of 17 January 2025, meaning that financial entities must comply with DORA as of that date. In respect of contracting compliance, financial entities must have renegotiated existing contracts in scope of DORA to comply at or before that date and all future contracts must comply as well.

DORA deals with digital resilience and therefore exclusively with work processes, policies and procedures, and contracts related to information and communications technology ("**ICT**"). According to DORA, "ICT services" is defined as *"digital and data services provided through ICT systems to one or more internal or external users 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"*. DORA does not provide further information or breakdown of what is considered "ICT services".

Consequently, the following cumulative conditions must be fulfilled for DORA to apply to a particular contract: The services must be

i. "digital and data services"
ii. "provided through ICT systems"
iii. "to one or more internal or external users"
iv. "on an ongoing services" nature

The main purpose of DORA is to establish high and robust digital resilience in the finance sector by stating both broad and concrete requirements in respect of:

- ICT risk management
- Reporting of major ICT, security, or payment-related incidents
- Resilience testing
- Information and intelligence gathering on cyber threats and vulnerabilities.

The contracting requirements is a minor part of the overall requirements covered in three out of 63 articles in DORA.

Technical standards and policy products under DORA

DORA contains 106 recitals in the preamble and 64 articles. To operationalize the use of DORA, the European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) are mandated through their joint committee to issue several binding policy products, so-called Regulatory Technical Standards ("**RTSs**"), Implementation Technical Standards ("**ITSs**"), and other joint guidelines, which have been published in two separate batches. The first batch of such policy products was published on 19 June 2023 and is currently pending final confirmation by the European Commission. The second batch was published on 8 December 2023 and the ESAs expect to submit the policy products to the European Commission and issue the guidelines by the deadline 17 July 2024 (exactly six months prior to DORA becoming effective across EU on 17 January 2025). The European Commission will issue the policy products in the form of Delegated Regulations that will be directly binding and will not require implementation by local law.

The contents of the RTSs and other guidelines will be key in creating and implementing internal policies, work processes, and artefacts to underpin DORA compliance.

The RTSs and guidelines include:

Title	DORA references	Contents
Estimation of aggregated annual costs and losses caused by major ICT-related incidents	Article 11	Sets out the harmonisation of the estimation by financial entities of their aggregated annual costs and losses caused by major information and communication technology.
Harmonise ICT risk management tools, methods, processes and policies	Articles 15 and 16	Sets out the harmonisation of ICT risk management tools, methods, processes and policies and develops a simplified ICT risk management framework for certain financial entities.
Criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats	Articles 18 and 19	Sets out detailed classification criteria, definitions relevant to the reporting of major incidents.
Content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents	Article 18, 19 and 20	Sets out the content of the reports for ICT related incidents and the notification for significant cyber threats, and the time limits for FEs to report these incidents to competent authorities.
Specifying elements related to threat led penetration tests	Article 26(11)	Sets out criteria for identifying financial entities required to conduct threat-led penetration testing, stipulates standards for internal testers, delineates testing phases, methodologies, results, and remediation processes, and specifies the necessary supervisory cooperation for implementing and mutually recognising TLPT.
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	Article 28	Sets out detailed content of the policy on the contractual arrangements regarding on the use of ICT services supporting critical or important functions provided by ICT third-party service providers.

Title	DORA references	Contents
Specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions	Article 30	Sets out requirements for the use of subcontracted ICT services supporting critical or important functions or material parts thereof by ICT third-party service providers and requirements regarding the implementation, monitoring and management of contractual arrangement regarding the subcontracting conditions for the use of ICT services.
Oversight cooperation and information exchange between the ESAs and the competent authorities	Article 32(7) and the articles in Section II of Chapter V	Sets out the cooperation between the ESAs and the CAs covering the detailed procedures and conditions for the allocation and execution of tasks between CAs and the ESAs and the details on the exchanges of information which are necessary for CAs to ensure the follow-up of recommendations addressed to CTPPs.
Harmonisation of conditions enabling the conduct of the oversight activities	Article 41	Sets out the information required from ICT third-party service providers and outlines the criteria for establishing a joint examination team and details the assessment process by competent authorities of measures implemented by CTPPs.

The draft RTSs are available on ESMAs website.[2]

Scope and key differences between DORA, EBA Outsourcing Guidelines and EIOPA Cloud Outsourcing Guidelines

We are providing a separate and detailed guidance note on the scope/applicability of DORA and the elements that financial entities should consider for a specific contract when assessing whether DORA, EBA Outsourcing Guidelines and/or EIOPA Outsourcing Guidelines apply.

There are many similarities between the approach taken under the EBA Outsourcing Guidelines, the EIOPA Cloud Outsourcing Guidelines, and the requirements under DORA. As an example, the pre-contract assessment requirements are broadly similar.

The well-known concepts of *"critical or important functions"* and proportionality apply in a similar manner to requirements under DORA. However, while EBA Outsourcing Guidelines and DORA have similar contracting requirements, DORA has more requirements that apply to all contracts, irrespective whether critical or important, where the same requirements under the EBA Outsourcing Guidelines and DEO only apply to contracts on critical and important functions. In practice and for purposes of contract compliance projects, this means that financial entities will have to institute several new contractual requirements in respect of contracts that during EBA contract compliance projects were designated as "non-critical and important" and which therefore previously were updated to meet less robust standards. In other words, when updating contracts to be DORA compliant there will be less work associated with updating those contracts that were originally designated as critical or important than the other on-going ICT contracts. The long tail of contracts to be updated has gotten longer.

The EBA Outsourcing Guidelines and EIOPA Cloud Outsourcing Guidelines cover outsourcing of *ongoing services* and neither cover one time delivery projects, nor functions which would normally fall outside the scope of what a financial entity can reasonably perform.

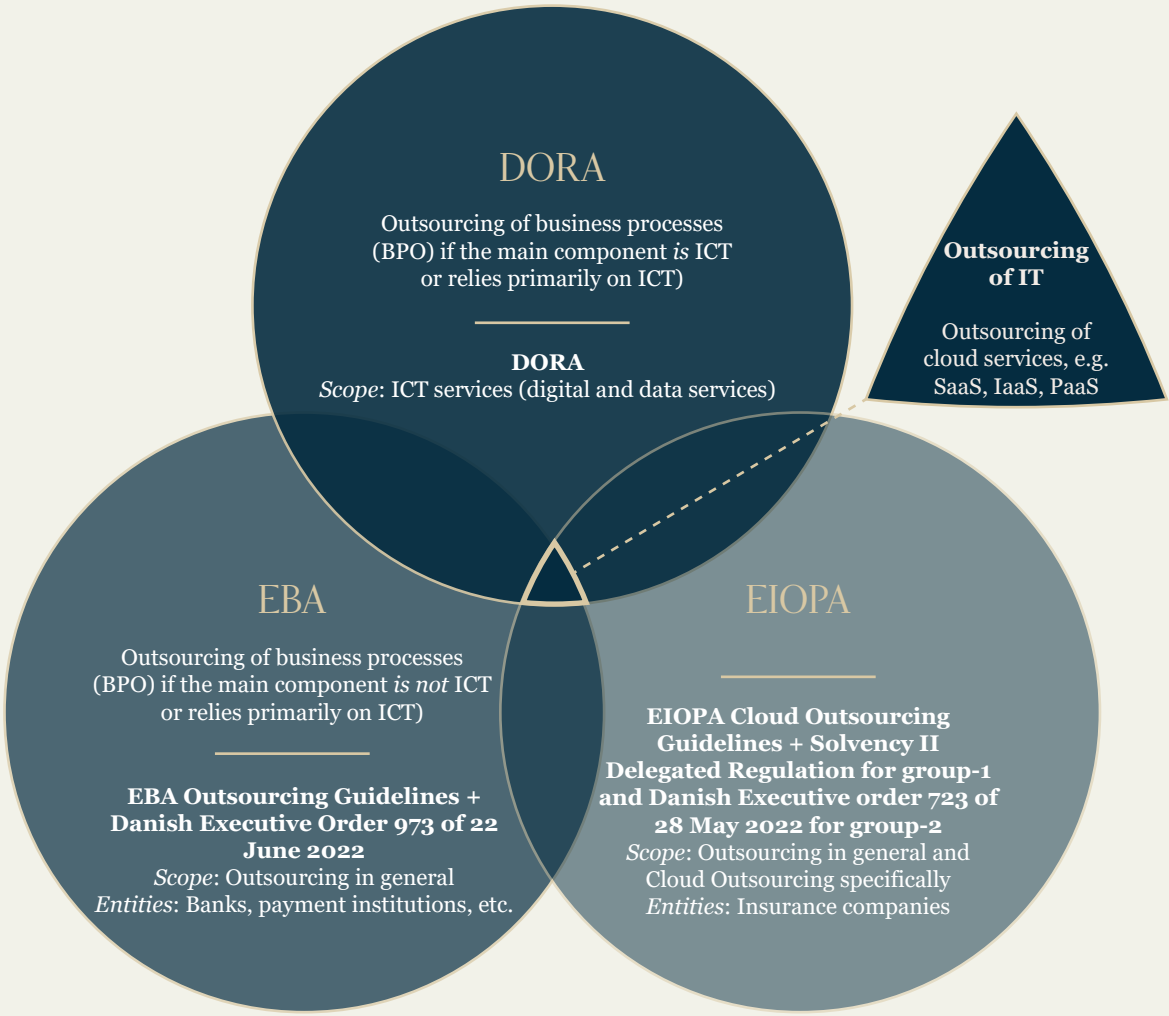
DORA applies to all ICT contracts concerned with the delivery of recurring services, including IaaS, PaaS, and SaaS services. As a starting point, the scope of EBA/EIOPA and DORA will overlap when dealing with ongoing services related to operation or maintenance of information technology.

The EBA criteria on services that *"normally fall outside the scope of what a financial institution"* does not apply under DORA. This means that contracts that may not be in-scope of the EBA Outsourcing Guidelines could be in-scope of DORA because the "normally fall outside" qualification does not apply under DORA.

2 https://www.esma.europa.eu/press-news/esma-news/esas-publish-first-set-rules-under-dora-ict-and-third-party-risk-management and https://www.esma.europa.eu/press-news/esma-news/esas-launch-joint-consultation-second-batch-policy-mandates-under-digital

For practical purposes, financial entities must reassess whether certain contracts were excluded from EBA contracting compliance projects for latter reason and if so, such contracts will likely be in-scope of a DORA contracting compliance project.

The overlapping regulatory scope



Sourcing/outsourcing of IT services

- DORA relates specifically to IT.
- Outsourcing of IT for banks etc. will be subject to DORA + EBA Outsourcing Guidelines.
- Outsourcing of cloud for insurance companies will be subject to DORA + EIOPA Cloud Outsourcing Guidelines.

The contractual requirements of DORA are complementary to the sectoral law applicable to outsourcing (DORA recital no. 69).

Sourcing/outsourcing of other services than IT

- Outsourcing of business processes (BPO) for banks etc. will likely be subject to EBA Outsourcing Guidelines and not DORA.

The contractual requirements of the sectoral law applicable to outsourcing will apply depending on the institution (bank, insurance company, etc.).

Key points:

- DORA applies to all ICT services provided on an ongoing basis via ICT systems. Services do not need to qualify as an "outsourcing".
- EBA and EIOPA also apply to outsourcings and cloud services, respectively, that do not involve ICT, e.g. BPO. It needs to qualify as an "outsourcing".
- Note that DORA, EBA and EIOPA all apply at the same time where the scope overlaps. This means that the principles under each relevant set of rules must be complied with (in other words, the accumulated standards).

Another important major difference between the EBA Outsourcing Guidelines and EIOPA Cloud Outsourcing Guidelines and DORA is that technical and process requirements under DORA are more elaborate, detailed, and prescriptive.

Where the guidelines established a framework, DORA designate to a (much) higher extent how a work process must be conducted, what a report must look like, which exact data are required to fulfil a given purpose etc.

This approach entails that it will be difficult to ensure and remain compliant unless a financial entity's work processes and artefacts created as part of such work processes are narrowly tailored to the concrete DORA and RTS requirements.

From a practical contract compliance perspective this means that:

- Work process requirements, such as reporting formats and similar, must be anchored in contracts with ICT providers to enable the customer (the financial entity) to be compliant.
- Renegotiations will likely take place at a time when the RTSs may not be final and therefore relevant contract mechanisms must be built-in to cover known requirements and cater for last moment changes.

Direct and indirect contracting requirements

Article 30 of DORA sets out approximately 20 explicit contracting requirements, such as "shall include [...] the right to monitor [...].". We call such contracting requirements for "**direct**" requirements. All direct contract requirements are listed in annex A to this guidance note. Annex A compares DORA's direct contracting requirements with the EBA Outsourcing Guidelines and pinpoints the gaps on direct contracting requirements that contracts must address to achieve full DORA compliance. The purpose is of this approach is that financial entities can focus any "upgrading" of EBA Outsourcing Guidelines compliant contracts on the gaps between the two sets of regulations, rather than starting all over.

When comparing the gaps between the EBA Outsourcing Guidelines and DORA in respect of explicit and direct contracting requirements, there are only few significant additions to be made. As mentioned, our initial view is explained in Annex A. Obviously, concrete guidance has not yet been issued by regulators and therefore our guidance is at this stage based on current assessments that may need updating or refinement over time. The purpose of this guidance is not to provide concrete legal advice, rather to provide our current thinking for purposes of further dialogue and development of approaches to securing compliant contracting.

In addition, DORA sets out several "**indirect**" requirements. These are elements that must be included in an ICT contract because without such elements the financial entity would not be able to fulfil a requirement applicable to the financial entity, hence the "indirect" nature.

Article 10(2) of the RTS on Harmonisation of ICT Risk Management Tools, Methods, Processes and Policies is an example of an indirect contract requirement. It states that *"These procedures shall: [...] ensure that the ICT third-party providers handle any vulnerabilities related to the ICT services provided to the financial entity and report them to the financial entity."* To ensure the ability of the financial entity to be compliant in real life, the contract with an ICT service provider must spell out the concrete handling and reporting requirements.

Another more circumvent example is article 1 of the same RTS that states that *"Financial entities shall ensure that the ICT security policy [...] sets out the consequences of non-compliance with the policies from staff of the financial entity and ICT third-party service providers [...]."*. To be compliant with this requirement an ICT security policy must as a starting point include the prescribed contents. However, compliance is not intended to be merely a paper-based exercise, therefore the indirect effect of the policy requirement is that a contract with the service provider must also include a relevant consequence, in other words a contractual right or remedy.

The concept of indirect contracting requirements significantly enlarges the scope of the contractual requirements that must be catered for when updating existing contracts or entering into new ones. A financial entity must elect to address only the direct contracting requirements and may on that basis appear to be compliant. But in that case there is a material risk that the contract with an ICT service provider is unaligned with the financial entity's regulatory requirements and that the misalignment will lead to separately payable change requests.

As part of our preparation of DORA templates and tools we have compiled a detailed overview of indirect contracting requirements that we will share with financial entities embarking on compliance projects. Some of those requirements are ideally captured by sweep clauses referring to relevant these or types of requirements, other requirements require specific wording. The choice on drafting strategy should largely be determined by seeking to avoid unnecessary risk premiums in your ICT contracts.

Contract compliance implementation strategies

Ensuring DORA contracting compliance in respect of *existing* contracts can be pursued through different strategies, including:

Existing contracts:

- **Greenfield approach:** Issue a template amendment to relevant service providers covering all DORA contracting requirements irrespective of overlap with EBA or EIOPA requirements.
- **Overlap approach:** Issue a template amendment to relevant service providers covering only the gap between the similar contracting requirements under the EBA Outsourcing Guidelines or EIOPA Cloud Outsourcing Guidelines.
  For certain service providers it may be prudent to base the compliance update on the service providers' standard amendment. Generally, only the larger ICT providers and in particular the hyperscalers and largest SaaS providers will develop their own standard amendments. Google Cloud and Oracle Cloud have each published overviews that set out how their standard contracts comply with DORA contracting requirements. Those overview documents are available on Oracles website.[3] Neither of the standard sets of terms cover the indirect contracting requirements.

New contracts:

- If based on **buy-side template:** Issue complete contract bundle which is "DORA, EBA, and EIOPA" compliant.
- If based on standard **sell-side template *without* financial services (FS) amendment:** Issue standard amendment which is "DORA, EBA, and EIOPA" compliant.
- If based on standard **sell-side template *with* financial services (FS) amendment:** Provide mark up to the FS amendment.

3 https://www.oracle.com/uk/a/ocom/docs/contract-checklist-dora.pdf and https://www.oracle.com/uk/a/ocom/docs/contract-checklist-for-eba-eiopa-esma-guidelines.pdf.

The DORA contracting process: Risk assessments and conduct of service provider due diligence

DORA contains requirements on risk assessment and service provider due diligence.

Financial entities should take into account that management of ICT third-party risk in general shall be implemented in light of the principle of proportionality. As part of exercising this principle, the institutions shall according to article 28(b) consider *"the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers, 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".*

DORA also requires institutions to maintain and update a register of information in relation to all contractual arrangements on the use of ICT services, which evidently requires that all relevant information is collected on service providers in its supply chain.

Consequently, risk assessment and proper due diligence is a fundamental and important part of DORA compliance.

Risk assessments

Chapter II of DORA concerns ICT risk management in general. This includes various ongoing risk assessments and identification of risks relating to the use of ICT services and dependencies on ICT third-party service providers (see article 8 of DORA).

With respect to the pre-contractual phase, DORA requires that the financial entity identify and assess all relevant risks before entering into a contractual arrangement on the use of ICT services. This should take into account ICT concentration risk at entity level.

As part of DORA's general principles for a sound management of ICT third-party risk, article 28(4)(c) of DORA requires:

> *"Before entering into a contractual arrangement on the use of ICT services, financial entities shall: […]*
>
> *(c)* ***identify and assess all relevant risks*** *in relation to the contractual arrangement, including the possibility that such contractual arrangement may contribute to reinforcing ICT concentration risk as referred to in Article 29; […]"*

The assessment of ICT concentration risk at entity level is further described in article 29(1) of DORA:

> *"When performing the identification and assessment of risks referred to in* ***Article 28(4), point (c)****, financial entities* ***shall also take into account*** *whether the envisaged conclusion of a contractual arrangement in relation to ICT services supporting critical or important functions would lead to any of the following:*
>
> *(a) contracting an ICT third-party service provider that is not easily substitutable; or*
>
> *(b) having in place multiple contractual arrangements in relation to the provision of ICT services supporting critical or important functions with the same ICT third-party service provider or with closely connected ICT third-party service providers.*
>
> *Financial entities shall weigh the benefits and costs of alternative solutions, such as the use of different ICT third-party service providers, taking into account if and how envisaged solutions match the business needs and objectives set out in their digital resilience strategy."*

Similar requirements apply when comparing with EBA Outsourcing Guidelines, including the focus on concentration risks.

Consequently, the essence of the DORA requirements is:

- A risk assessment may lead to the conclusion that ICT services should not be sourced via a third party.
- Risk assessment must be made before entering into the contractual arrangement on ICT services, re-visited at relevant intervals, and updated if events occurring merits an update.
- Risk assessments will in practice be closely connected to an institution's business- and service continuity planning and to its documented exit plans.
- Risk assessments must take the vendor due diligence made into consideration.
- A risk assessment is done on per contract basis.
- The financial entity must take into account the risk of relying on one of very few vendors.

Due diligence

With respect to the pre-contractual phase, DORA requires that the financial entity to conduct proper due diligence in the process of selection and assessment of ICT third-party service providers and assessing potential conflicts of interest.

As part of DORA's general principles for a sound management of ICT third-party risk, article 28(4)(d) and (e) of DORA requires:

> *"Before entering into a contractual arrangement on the use of ICT services, financial entities shall: […]*
>
> *(d)* ***undertake all due diligence*** *on prospective ICT third-party service providers and ensure throughout the selection and assessment processes that the ICT third-party service provider is suitable;*
>
> *(e)* ***identify and assess conflicts of interest*** *that the contractual arrangement may cause."*

Similar requirements apply when comparing with EBA Outsourcing Guidelines.

Consequently, the essence of the DORA requirements is:

- A vendor due diligence can be based on a template and should follow a chosen methodology but the due diligence must take all relevant individual circumstances into consideration.
- In reality, the due diligence must be based on a very broad business assessment taking the proportionality principle into consideration.
- A renewed due diligence must be made if more contracts are to be entered into with the same vendor. Such new due diligence can be in the form of a verification of the applicability of a previously made due diligence.

How we can assist you

Gorrissen Federspiel advises financial entities on DORA compliance in general and on contracting compliance programmes. As part of our advisory we provide access to a range of tools that include:

- Gorrissen Federspiel's scope agnostic outsourcing framework agreement for financial entities, which comply with EBA/DORA/ESMA/EIOPA requirements out of the box
- Best practice guidance notes as released from time to time
- Training presentations
- EBA and DORA compliance project guidance
- EBA Outsourcing Guidelines compliance tracker covering all process and other requirements
- EBA Outsourcing and C/I assessment tool
- DORA Contract and C/I assessment tool
- Combined EBA, EIOPA, and DORA Contract and C/I assessment tool
- Gap analysis EBA Outsourcing Guidelines and DORA contracting requirements
- Gap analysis EIOPA Guidelines on outsourcing to cloud service providers and DORA contracting requirements
- Overview of indirect DORA contracting requirements

Contact

Ole Horsfeldt
Partner

T +45 33 41 43 65 | M +45 24 28 68 40
oho@gorrissenfederspiel.com

Christoffer Stensdal
Digital Business Counsel

T +45 33 41 42 55 | M +45 26 28 43 98
cst@gorrissenfederspiel.com

Morten Nybom Bethe
Partner

T +45 33 41 41 14 | M +45 40 31 89 42
mnb@gorrissenfederspiel.com

Christian Aaby Köhler
Managing Counsel

T +45 33 41 41 13 | M +45 26 19 42 68
cla@gorrissenfederspiel.com

Tue Goldschmieding
Partner

T +45 33 41 42 03 | M +45 24 28 68 75
tgg@gorrissenfederspiel.com

Jarl Phillip Øster
Senior Digital Business Counsel

T +45 33 41 41 78 | M +45 24 28 68 24
jao@gorrissenfederspiel.com

Annex A - Direct DORA contracting requirements compared with EBA Outsourcing Guidelines

The table below sets out the direct DORA contracting requirements and maps where those requirements are covered, if that is the case, in the EBA Outsourcing Guidelines and in DEO.

The "gap" column sets out the particular DORA requirement is not fully covered by an EBA or DEO requirement. The intention is to identify elements where a template DORA amendment should replace or supplement terms and conditions agreed in an existing agreement which is EBA/DEO compliant.

The table is based on DORA and the draft Regulatory Technical Standard on subcontracting.

No.	DORA art. ref	DORA requirement	EBA/DEO	Gap
1.	28, 3	*"The contractual arrangements referred to in the first subparagraph shall be appropriately documented, …*	No similar requirement	This is not a real gap as this requirement is generally complied with by having a writing contract.
2.	28, 7	*"Financial entities shall ensure that contractual arrangements on the use of ICT services may be terminated in any of the following circumstances: (a) significant breach by the ICT third-party service provider of applicable laws, regulations or contractual terms; (b) circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the ICT third-party service provider; (c) ICT third-party service provider's evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and, confidentiality, of data, whether personal or otherwise sensitive data, or non-personal data; (d) where the competent authority can no longer effectively supervise the financial entity as a result of the conditions of, or circumstances related to, the respective contractual arrangement."*	EBA 98 DEO annex 3, 5	There is no general gap between DORA and EBA and the termination rights must apply to all contracts irrespective of criticality. However, under DEO the requirement only applies to critical or important contracts. We suggest using the relevant DORA wording for all ICT and outsourcing contracts. The DORA wording under b) focuses on termination due to material changes that has been identified through monitoring of ICT third-party risk, whereas the EBA/DEO wording only "where there are existence of material changes". We suggest using the DORA wording which will also cover the EBA and DEO requirement. The DORA wording under c) has a similar scope as the EBA requirement but the DORA wording is possibly broader. We suggest using the DORA wording.
3.	30, 1	*"The rights and obligations of the financial entity and of the ICT third-party service provider shall be clearly allocated and set out in writing"*	EBA 74 DEO 21	No gap.
4.	30, 1	*"The full contract shall include the service level agreements"*	EBA 75 i) DEO annex 3, 1 l (i)	No gap
5.	30, 1	*"and be documented in one written document which shall be available to the parties on paper, or in a document with another downloadable, durable and accessible format."*	No similar requirement	This is a process requirement that enables the buy-side to require that all terms and conditions available online can be downloaded in one file (one written document).

No.	DORA art. ref	DORA requirement	EBA/DEO	Gap
6.	30, 2 a)	*"a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, indicating whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting;"*	EBA 75 a) and e) DEO annex 3, 1 a) and f)	The only difference in requirements is that descriptions under DORA must also be "complete". For practical purposes, this "gap" is not an element which is managed by a concrete contract provision. Rather, this is a process requirement which can be interpreted to mean that the description of services must be in place at the time of signing and cannot (which it is seen from time to time) be developed after signing other than a relevant detailing of time plans and similar.
7.	30, 2 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 thirdparty service provider to notify the financial entity in advance if it envisages changing such locations;"*	EBA 75 f) DEO annex 3, 1 g) and h)	No gap, except for the following. Note that EBA and DEO requirement only applies to critical and important functions but the DORA requirement applies to all contracts.
8.	30, 2 c)	*" provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data"*	EBA 75 g) DEO annex 3, 1 i)	Note that EBA and DEO requirement only applies to critical and important functions but the DORA requirement applies to all contracts. The EBA requirement is subject to "where relevant". The same qualification does not apply explicitly under DORA. We suggest using the DORA wording.
9.	30, 2 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 third-party service provider, or in the event of the termination of the contractual arrangements;"*	EBA 75 m9 DEO annex 3, 1 0)	Note that EBA and DEO requirement only applies to critical and important functions but the DORA requirement applies to all contracts. The DORA requirement has added requirements as to access "in an easily accessible format". We suggest using the DORA wording.
10.	30, 2 e)	*"service level descriptions, including updates and revisions thereof"*	EBA 75 i) DEO annex 3, 1 l) (i)	No gap.
11.	30, 2 f)	*"the obligation of the ICT third-party service provider 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"*	No similar requirement	This requirement is specific to DORA and represents a gap to be dealt with.

No.	DORA art. ref	DORA requirement	EBA/DEO	Gap
12.	30, 2 g)	*"the obligation of the ICT third-party service provider to fully cooperate with the competent authorities and the resolution authorities of the financial entity, including persons appointed by them"*	75 n) DEO annex 3, 1 p)	No gap, except for the following. Note that EBA and DEO requirement only applies to critical and important functions but the DORA requirement applies to all contracts.
13.	30, 2 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;"*	No similar requirement	This requirement does not represent a gap. Rather, this is requirement for financial entities to consider which termination rights and associated notice periods will fulfil expectations of competent authorities.
14.	30, 2 i)	*"the conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programmes and digital operational resilience training in accordance with Article 13(6)"*	No similar requirement	This requirement is specific to DORA and represents a gap to be dealt with.
15.	30, 3 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"*	EBA 75 i) DEO annex 3, 1 l (i)	There is no gap in respect of the requirements as to service descriptions and service levels. DORA has a new requirement stating that a contract must "enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met". This requirement should be backed up by concrete wording referring to customary remedies such as service credits, proportionate reduction, and the duty to remediate.
16.	30, 3 b)	*"notice periods and reporting obligations of the ICT third-party service provider to the financial entity, including notification of any development that might have a material impact on the ICT third-party service provider's ability to effectively provide the ICT services supporting critical or important functions in line with agreed service levels"*	EBA 75 j) DEO annex 3, 1 k)	No gap.
17.	30, 3 c)	*"requirements for the ICT third-party service provider 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"*	EBA 75 l) DEO annex 3, 1 n)	The DORA wording is more expansive and refers also to "to have in place ICT security measures, tools and policies". We suggest using the broader DORA wording.
18.	30, 3 d)	*"the obligation of the ICT third-party service provider to participate and fully cooperate in the financial entity's TLPT as referred to in Articles 26 and 27"*	No similar requirement	This requirement is specific to DORA and represents a gap to be dealt with.

No.	DORA art. ref	DORA requirement	EBA/DEO	Gap
19.	30, 3 e) (i)	*"the right to monitor… the following: 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 third-party service provider, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies "*	EBA 75 h) DEO annex 3, 1 j) EBA 85-89 (on audit) DEO annex 3, 4 a)-d)	The DORA requirements are more expansive than the EBA requirements. We suggest developing new contract provisions that full cover the scope of both EBA and DORA requirements.
20.	30, 3 e) (ii)	*"the right to monitor… the following: the right to agree on alternative assurance levels if other clients' rights are affected "*	No similar requirement	This requirement is specific to DORA and represents a gap to be dealt with.
21.	30, 3 e) (iii)	*"the right to monitor… the following: the obligation of the ICT third-party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, financial entity or an appointed third party "*	EBA 75 n) DEO annex 3, 1 p)	In principle there is no gap, but the list of authorities needs to be updated.
22.	30, 3 e) (iv)	*"the right to monitor… the following: the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits "*	No similar requirement	This requirement is specific to DORA and represents a gap to be dealt with.
23.	30, 3 f (i)	*"exit strategies, in particular the establishment of a mandatory adequate transition period: during which the ICT third-party service provider 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"*	EBA 99 DEO annex 3, 6 a-c)	No gap.
24.	30, 3 f (ii)	*"exit strategies, in particular the establishment of a mandatory adequate transition period: allowing the financial entity to migrate to another ICT third-party service provider or change to in-house solutions consistent with the complexity of the service provided"*	EBA 99 DEO annex 3, 6 a-c)	No gap.
25.	RTS on subcontracting 4 a)	*"In particular, and without prejudice to the final responsibility of the financial entity, for each ICT service eligible for subcontracting the written contractual agreement shall specify: that the ICT third-party service provider is required to monitor all subcontracted ICT services supporting a critical or important function to ensure that its contractual obligations with the financial entity are continuously met"*	EBA 78 c) DEO annex 3, 2 c)	No gap

No.	DORA art. ref	DORA requirement	EBA/DEO	Gap
26.	RTS on subcontracting 4 b)	*In particular, and without prejudice to the final responsibility of the financial entity, for each ICT service eligible for subcontracting the written contractual agreement shall specify: the monitoring and reporting obligations of the ICT third-party service provider towards the financial entity;*	No similar requirement (in respect of reporting in the specific context of subcontracting)	This requirement is specific to DORA and represents a gap to be dealt with.
27.	RTS on subcontracting 4 c)	*In particular, and without prejudice to the final responsibility of the financial entity, for each ICT service eligible for subcontracting the written contractual agreement shall specify: that the ICT third-party service provider shall assess all risks, including ICT risks, associated with the location of the potential subcontractor and its parent company and the location where the ICT service is provided from*	No similar requirement	This requirement is specific to DORA and represents a gap to be dealt with.
28.	RTS on subcontracting 4 d)	*In particular, and without prejudice to the final responsibility of the financial entity, for each ICT service eligible for subcontracting the written contractual agreement shall specify: the location and ownership of data processed or stored by the subcontractor, where relevant;*	No similar requirement specific to subcontractors but in principle included under EBA 75 f) DEO annex 3, 1 g)	Not necessarily a gap but we suggest to include references to subcontractors in respect of the specification of "the location and ownership of data processed or stored".
29.	RTS on subcontracting 4 e)	*In particular, and without prejudice to the final responsibility of the financial entity, for each ICT service eligible for subcontracting the written contractual agreement shall specify: that the ICT third-party service provider is required to specify the monitoring and reporting obligations of the subcontractor towards the ICT third-party service provider, and where relevant, towards the financial entity*	No similar requirement	This requirement is specific to DORA and represents a gap to be dealt with.
30.	RTS on subcontracting 4 f)	*In particular, and without prejudice to the final responsibility of the financial entity, for each ICT service eligible for subcontracting the written contractual agreement shall specify: that the ICT third-party service provider is required to ensure the continuous provision of the ICT services supporting critical or important functions, even in case of failure by a subcontractor to meet its service levels or any other contractual obligations;*	No similar requirement	This requirement is specific to DORA and represents a gap to be dealt with.

No.	DORA art. ref	DORA requirement	EBA/DEO	Gap
31.	RTS on subcontracting 4 g)	*In particular, and without prejudice to the final responsibility of the financial entity, for each ICT service eligible for subcontracting the written contractual agreement shall specify: the incident response and business continuity plans in accordance with Article 11 of Regulation (EU) 2022/2554 and service levels to be met by the ICT subcontractors;*	No similar requirement	This requirement is specific to DORA and represents a gap to be dealt with.
32.	RTS on subcontracting 4 h)	*In particular, and without prejudice to the final responsibility of the financial entity, for each ICT service eligible for subcontracting the written contractual agreement shall specify: the ICT security standards and any additional security features, where relevant, to be met by the subcontractors in line with the RTS mandated by Article 28(10) of Regulation (EU) 2022/2554;*	No similar requirement	This requirement is specific to DORA and represents a gap to be dealt with.
33.	RTS on subcontracting 4 i)	*In particular, and without prejudice to the final responsibility of the financial entity, for each ICT service eligible for subcontracting the written contractual agreement shall specify: that the subcontractor shall grant to the financial entity and relevant competent and resolution authorities at least the same audit, information and access rights as 13 granted to the financial entity and relevant competent authorities by the ICT thirdparty service provider;*	EBA 79 b) DEO annex 3, 2 i)	No gap.
34.	RTS on subcontracting 4 j)	*In particular, and without prejudice to the final responsibility of the financial entity, for each ICT service eligible for subcontracting the written contractual agreement shall specify: that the financial entity has termination rights in accordance with article 7, or in case the provision of services fails to meet service levels agreed by the financial entity*	No similar requirement	This requirement is specific to DORA and represents a gap to be dealt with.
35.	RTS on subcontracting 6, 1)	*In case of any material changes to the subcontracting arrangements, the financial entity shall ensure, through the ICT contractual arrangement with its ICT third-party service provider, that it is informed with a sufficient advance notice period to assess the impact on the risks it is or might be exposed to, in particular where such changes might affect the ability of the ICT third-party service provider to meet its obligations under the contractual agreement, and with regard to changes considering the elements listed in Article 1.*	EBA 78 e) DEO DEO annex 3, 2 f)	No gap.

No.	DORA art. ref	DORA requirement	EBA/DEO	Gap
36.	RTS on subcontracting 6, 3)	*The financial entity shall require that the ICT third-party service provider implements the material changes only after the financial entity has either approved or not objected to the changes by the end of the notice period.*	No similar requirement (the existing requirement in EBA 78 f) and DEO Annex 3, 2 g) is scoped slightly differently	This requirement is specific to DORA and represents a gap to be dealt with.
37.	RTS on subcontracting 6, 4)	*The financial entity shall have a right to request modifications to the proposed subcontracting changes before their implementation if the risk assessment referred to referred to in paragraph 1) concludes that the planned subcontracting or changes to 14 subcontracting by the ICT third-party service provider exposes the financial entity to risks as specified in Article 3(1) that exceed its risk appetite.*	No similar requirement	This requirement is specific to DORA and represents a gap to be dealt with.
38.	RTS on subcontracting 7, 1) a)	*Without prejudice to the termination clauses set out in accordance with Article 28 paragraph (10) of Regulation (EU) 2022/2554, the financial entity has a right to terminate the agreement with the ICT third-party service provider in each of the following cases:* *when the ICT third-party service provider implements material changes to subcontracting arrangements despite the objection of the financial entity, or without approval within the notice period as referred to in Article 6,*	Partly covered by EBA 79 g) and DEO Annex 3, 2 h)	Must be dealt with by appropriate additional drafting.
39.	RTS on subcontracting 7, 1) b)	*Without prejudice to the termination clauses set out in accordance with Article 28 paragraph (10) of Regulation (EU) 2022/2554, the financial entity has a right to terminate the agreement with the ICT third-party service provider in each of the following cases:* *when the ICT third-party service provider subcontracts an ICT service supporting a critical or important function explicitly not permitted to be subcontracted by the contractual agreement.*	No similar requirement (though in principle covered by the broader wording of EBA 79 g) and DEO Annex 3, 2 h)	We suggest to include drafting explicitly tailored to meet the DORA requirement.

Gorrissen Federspiel
Axeltorv 2
1609 Copenhagen V
Denmark

gorrissenfederspiel.com