3.2 Classification of ICT systems and information

As described in section 2.1, ICT systems and information used in business functions must be identified and classified. The interactions between the ICT assets and links to the business functions must also be taken into account (Art. 8 para. 1 DORA in conjunction with Art. 4 RTS RMF). This procedure combines the previous separate definition of an information network and the listing of the components of the IT systems (Chapters 3 and 8 BAIT/VAIT) and thus creates a holistic picture of the ICT systems and information, which was not previously available in this form.

3.3 Extension to all changes to ICT systems

The risk-oriented approach to change management already familiar from sections 8.4 and 8.5 BAIT/VAIT is required in DORA in an extended form (Art. 9 para. 4 lit. e, f DORA in conjunction with Art. 17 RTS RMF). The previous approach was limited to significant changes, this restriction will no longer apply in future. According to Art. 9 para. 4 lit. e DORA, all changes to ICT systems within the scope of the ICT change management in a controlled manner, to record, test, evaluate, approve, implement and review. This means that a significantly larger number of changes need to be considered than before.

Furthermore, Art. 17 RTS RMF specifies the minimum content of the ICT change management procedure, such as testing obligations, testing of these changes, impact analyses or fallback solutions, and thus goes beyond the previous requirements. Further information on this follows in section 5.3 from the project management perspective.

3.4 Separate data storage and synchronisation of data backup

The topic of data backup should already be known from the data backup concept required in section 8.7 BAIT/VAIT. According to Art. 12 DORA, a guideline on backup procedures as well as procedures and methods for recovery and restoration must be defined. This extends the existing requirements of BAIT/VAIT, which primarily require a data backup concept.

DORA contains similar conceptual requirements to the familiar data backup concept (Art. 12 para. 1 lit. a DORA). Guidelines and procedures must be developed and documented to minimise downtimes when restoring ICT systems and data and to ensure limited disruptions and losses.

In addition, when carrying out data backup and recovery in accordance with Art. 12 para. 2 DORA, it must be ensured that the security of the network and information systems and the availability, authenticity, integrity or confidentiality of data is not jeopardised. This requirement is not included in the BAIT/VAIT, in particular with regard to the security of the systems (Chapter 8.7 BAIT/VAIT).

When dealing with source code from application development, the RTS RMF contains very specific requirements. For example, the source code must be checked for anomalies using static and dynamic test procedures prior to productive use (Art. 16 para. 3 RTS RMF). This also applies to source code created by third parties and proprietary software (compiled source code) (Art. 16 para. 8 RTS RMF).

Individual data processing (IDP) is only implicitly included in the RTS RMF. No distinction is made between IDP and purchased (standard) applications, but it is pointed out that developments outside the IT function must be checked for risks (Art. 16 para. 9 RTS RMF). Although the essential requirements for IDVs remain the same, the review may be more extensive than before due to the lack of special status of IDVs.

5.3 Removal of the materiality threshold in ICT change management

For ICT change management (Art. 17 RTS RMF), there are innovations compared to the existing requirements of BAIT/VAIT, particularly with regard to the assessment of changes to software, hardware, firmware, systems or security parameters (Art. 17 para. 1 RTS RMF). At this point, the perspective changes in particular, as the focus is now on data as an asset worthy of protection and the technology used (Art. 17 para. 1 RTS RMF). In contrast, the BAIT/VAIT consider the impact of the changes in the context of the entire IT organisation as part of an impact analysis. However, the RTS RMF contains specific requirements for the operational process for handling changes (Art. 17 para. 1 RTS RMF). Among other things, the separation of functions and roles is mentioned here (Art. 17 Para. 1 lit. b RTS RMF) for the approval of changes. The implementation of a specific process is not described or required.

Chapter 7.1 BAIT/VAIT previously stipulated that material changes must be subject to a prescribed analysis process and that other affected organisational units must be involved depending on the materiality of the changes. The RTS RMF no longer distinguishes between material and non-material changes. Therefore, in future, all changes to ICT systems must be recorded, tested, evaluated, authorised, implemented and reviewed in a controlled manner (Art. 17 para. 1 lit. c RTS RMF). The involvement of other organisational units provided for in the BAIT/VAIT is not explicitly required in the RTS RMF.

6. ICT third party risk management

This section sets out the requirements of Art. 1, 5 and Chapter V Section I (Art. 28 - 30) DORA, the RTS TPPol and the RTS-E-SUB for ICT third party risk management. management are compared with those of Chapter 9 of BAIT ("Outsourcing and other external procurement of IT services") and Chapter 9 of VAIT ("Outsourcing of IT services and other service relationships in the area of IT services"). Extracts from the minimum requirements for risk management (AT 9 MaRisk) and minimum requirements for the business organisation of insurance companies

TPPol[12]). This also applies to ICT third-party service providers that are themselves under supervision or are monitored (Art. 1 lit. g RTS TPPol).

Under DORA, there is a comprehensive and very specific consideration of concentration risks with the aim of identifying and appropriately monitoring them. For this purpose, in the case of contractual agreements that affect critical or important functions, it is determined and assessed whether the third-party ICT service provider could not be easily replaced or whether there are multiple purchases of ICT services from a third-party ICT service provider. If there are concentration risks, financial companies must weigh up the benefits and costs of alternative solutions (Art. 29 para. 1 DORA). This concentration risk is included both in the ex-ante risk analysis in accordance with Art. 5 RTS TPPol and in the analyses for subcontracting in accordance with Art. 3 para. 1 lit. h RTS-E SUB.

6.6 Changes to the governance of ICT third-party risk

There are also changes in the area of governance, in particular an increased involvement of the management body, e.g. through the review of ICT third-party risks (Art. 28 para. 2 DORA) or the approval of the guideline for the use of ICT services that support critical or important functions (Art. 5 para. 2 lit. h DORA and Art. 3 para. 1 RTS TPPol), as well as reporting channels for the use of ICT services (Art. 5 para. 2 lit. i DORA). A function for monitoring the agreements concluded with third-party ICT service providers on the use of ICT services must be established (Art. 5 para. 3 DORA, see also section 1.2), which is comparable to the (central) outsourcing officer.

6.7 Note on reporting obligations and information register

However, reporting obligations, in particular with regard to the information register, the annual report to the competent authorities and the notification of intended contractual agreements (Art. 28 para. 3 DORA) are not the subject of these implementation guidelines.

7. Operational Information security

This section compares the requirements for data and system security measures of Art. 9, 10 DORA and Art. 6, 7, 10, 11, 12, 13, 14, 22 and 23 RTS RMF with those of operational information security of Chapter 5 BAIT/VAIT.

For the area of operational information security in DORA, it should be noted that the level of detail of the requirements is significantly higher than previously in Chapter 5 BAIT/VAIT. The level of detail is more in line with the

[12] See recital 5 RTS TPPol in relation to affiliated institutions: "When applying the policy, ICT intra-group service providers, including those fully or collectively owned by financial entities within the same institutional protection scheme, should be considered as ICT third-party services providers."

8. Identity and rights management

This section compares the authorisation management requirements of Art. 18, 20 and 21 RTS RMF with those of authorisation management in Chapter 6 BAIT/VAIT.

With regard to the identity and rights management processes, it should be noted that DORA does not result in too many changes in terms of content compared to BAIT/VAIT. Familiar processes such as application, assignment and recertification remain as described in Chapter 6 BAIT/VAIT. With regard to identity and rights management, the existing requirements are even more detailed than those specified in RTS RMF Chapter II.

8.1 Explicit requirements for identity management

Specific requirements for identity management are set out in Art. 20 RTS RMF. This was not previously explicitly required in the BAIT/VAIT, but the content requirements f o r identity management, as the basis for access and admission management, were already in place. The effort required to adapt existing processes is likely to be minimal. According to Art. 20 RTS RMF, guidelines and procedures for identity management must be developed, documented and implemented. The guidelines must provide that

- each employee (including those of third-party ICT service providers) who accesses the financial organisation's information assets and ICT assets is assigned a unique identity,
- these assignments are also retained in the event of reorganisation and after the end of the contractual relationship and
- a lifecycle management process for identities and accounts is introduced, ideally using automated solutions.

8.2 Introduction of the "need-to-use" principle

In access management (Art. 21 RTS RMF), the "need-to-know" and "least privilege" principle from section 6.2 BAIT/VAIT is supplemented by the "need-to-use" principle. However, the newly introduced principle is reflected in the principle of economy in Chapter 6.2 BAIT/VAIT, meaning that increased costs are not to be expected here. It is also required, among other things, that

- the separation of functions is guaranteed,
- generic accounts are limited as far as possible so that activities can always be clearly assigned to an acting person and
- controls should be introduced to prevent unauthorised access.

There is an innovation in the area of recertification of authorisations. This should take place in a six-monthly cycle for all authorisations that affect critical or important functions (Art. 21 para. 1 lit. e point iv RTS RMF). For all other authorisations, an annual

rhythm. There is no need to differentiate between functional and technical access.

Privileged emergency or administrative access may only be granted on a "need-to-use" and ad-hoc basis. Where possible, automated solutions for privileged access management (Privileged Access Management - PAM) must be used. Privileged and remote access must be carried out with strong authentication (along leading practices) (Art. 21 para. 1 lit. f point ii RTS RMF).

III. Appendix

Minimum contract contents

This table contains an overview of the contractual content that must be agreed between the financial organisation and the third-party ICT service provider in accordance with DORA or the RTS TPPol and RTS-E SUB. Contractual components that should ideally be agreed but are not explicitly listed in the legal texts are not included in this list.

Topic	Contract content	Reference	Extract from the legal text	kwF[13]
Formal requirements	Written, permanently accessible document	Art. 30 para. 1 DORA	The rights and obligations of the Financial Enterprise and the Third Party ICT Service Provider are clearly assigned and set out in writing. The complete contract includes the service level agreement and is set out in a written document available to the parties in paper form or in a document in another downloadable, durable and accessible format. documented.	
Formal requirements	Written document with date and signature for significant changes	Art. 8 para. 4 RTS TPPol	The policy shall ensure that material changes to the contractual agreement are to be formalised in a written document which is dated and signed by all parties and shall specify the renewal process for the contractual arrangements.[14]	X
Description of the ICT service	Clear and complete description of all functions and ICT services	Art. 30 para. 2 lit. a DORA	a clear and complete description of all functions and ICT services to be provided by the third-party ICT service provider [...]	

[13] Labelling of the contractual requirements that are only necessary for ICT services that support critical or important functions (kwF).

[14] Presentation of the original English texts, as no German translation of the technical regulatory standards was available at the time the tables were created (as at 10 June 2024).

Topic	Contract content	Reference	Extract from the legal text	kwF[13]
Subcontracting	Permissibility of subcontracting ("which support critical or important functions or essential parts thereof") and conditions for subcontracting Subcontracting	Art. 30 para. 2 lit. a DORA	[...] specifying whether the subcontracting of ICT services supporting critical or important functions or essential parts thereof is authorised, and, if this is the case, whether the subcontracting of ICT services supporting critical or important functions or essential parts thereof is authorised. case - which conditions apply to this subcontracting	X
Location	Locations (regions or countries) of processing, storage and provision	Art. 30 para. 2 lit. b DORA	the locations - i.e. the regions or countries - where the contracted or subcontracted functions and ICT services are to be provided and where data to be processed, including the storage location, [...]	
Location	Notification of intended change of location	Art. 30 para. 2 lit. b DORA	[...] as well as the requirement for the ICT third-party service provider to to notify the finance company in advance if it intends to change these locations	
Security	Protection objectives, data protection provisions	Art. 30 para. 2 lit. c DORA	Provisions on availability, authenticity, integrity and confidentiality in relation to data protection, including the protection of personal data	
Data access	Ensuring access to data (e.g. in the event of insolvency), recovery and return	Art. 30 para. 2 lit. d DORA	Provisions on ensuring access to personal and non-personal data processed by the financial undertaking in the event of insolvency, liquidation, cessation of the ICT third-party service provider's business activities or termination of the contractual arrangements, and on the recovery and return of such data in an easily accessible form. accessible format	
Description of the ICT service	Service level descriptions, including updates and revisions	Art. 30 para. 2 lit. e DORA	Service level descriptions, including updates and revisions	
ICT incident	Support in the event of an ICT incident, determination of costs	Art. 30 para. 2 lit. f DORA	the obligation of the third-party ICT service provider to provide assistance to the financial undertaking in the event of an ICT incident related to the ICT service provided to the financial undertaking at no additional cost or at a cost to be determined in advance	
Supervision	Cooperation with competent authorities	Art. 30 para. 2 lit. g DORA	the obligation of the third-party ICT service provider to co-operate fully with the authorities and resolution authorities responsible for the financial undertaking, including the authorities and resolution authorities designated by these named persons	

Topic	Contract content	Reference	Extract from the legal text	kwF[13]
Cancellation	Cancellation rights and minimum notice periods in accordance with the expectations of the competent authorities	Art. 30 para. 2 lit. h DORA	Termination rights and associated minimum notice periods for the termination of contractual agreements in accordance with the expectations of the responsible authorities and the resolution authorities	
Training courses	Participation in awareness-raising and training sessions of the financial organisation on ICT security and digital operational resilience	Art. 30 para. 2 lit. i DORA	Conditions for the participation of third-party ICT service providers in the ICT security awareness and digital operational resilience training programmes offered by financial institutions pursuant to Art. 13 (6)	
Description of the ICT service	Complete description of the service level with precise quantitative and qualitative performance targets (including updates and revisions)	Art. 30 para. 3 lit. a DORA	complete service level descriptions, including updates and revisions, with precise quantitative and qualitative performance targets within the agreed service level to enable the financial organisation to effectively monitor ICT services and take appropriate corrective action without delay when a agreed quality of service is not achieved	X
Cancellation	Cancellation periods of the ICT third-party service provider	Art. 30 para. 3 lit. b DORA	notice periods and reporting obligations of the third-party ICT service provider to the financial undertaking, including reporting any developments that materially affect the ability of the third-party ICT service provider to provide ICT services in support of critical or important functions in accordance with the agreed service levels effectively, could have an impact on the	X
Reporting	Reporting obligations of the ICT third-party service provider	Art. 30 para. 3 lit. b DORA	notice periods and reporting obligations of the third-party ICT service provider to the financial undertaking, including reporting any developments that materially affect the ability of the third-party ICT service provider to provide ICT services in support of critical or important functions in accordance with the agreed service levels effectively, could have an impact on the	X
Business continuation management	Implementation and testing of emergency plans	Art. 30 para. 3 lit. c DORA	Requirements for the ICT third-party service provider to implement and test emergency plans [...]	X
Security	ICT security measures (appropriate level of security, in line with the financial organisation's legal framework)	Art. 30 para. 3 lit. c DORA	Requirements for the third-party ICT service provider [...] to have measures, tools and ICT security policies and guidelines in place that provide an appropriate level of security for the provision of services by the financial organisation in accordance with its legal framework;	X

Topic	Contract content	Reference	Extract from the legal text	kwF[13]
TLPT	Participation and involvement in TLPT[15]	Art. 30 para. 3 lit. d DORA	the obligation of the third party ICT service provider to participate in the TLPT of the financial undertaking referred to in Articles 26 and 27; and to co-operate fully	X
Monitoring	Right to continuously monitor the performance of the ICT third-party service provider	Art. 30 para. 3 lit. e DORA	the right to monitor the performance of the third-party ICT service provider on an ongoing basis	X
Inspection rights	Inspection rights for FU and supervision, including the right to make copies	Art. 30 para. 3 lit. e number i DORA	unrestricted access, inspection and audit rights of the financial undertaking or a delegated third party and the competent authority and the right to obtain copies of relevant documents on site if they are critical to the ICT third-party service provider's business, provided that the effective exercise of these rights is not hindered by other contractual arrangements or implementing directives, or is restricted	X
Inspection rights	Restriction of inspection rights if the rights of other customers are affected	Art. 30 para. 3 lit. e point ii DORA	the right to agree alternative confirmation levels if the rights of other customers are affected	X
Inspection rights	Unrestricted co-operation for on-site inspections and audits	Art. 30 para. 3 lit. e point iii DORA	the obligation of the ICT third-party service provider to co-operate fully with on-site inspections and audits carried out by the competent authorities, the lead supervisory authority, the financial undertaking or a contracted third party become	X
Inspection rights	Notification obligation for audit planning	Art. 30 para. 3 lit. e number iv DORA	the obligation to provide details of the scope and frequency of these inspections and the procedure to be followed in the process	X
Inspection rights	Exercise of audit rights by an independent third party for financial undertakings that are micro-entities	Art. 30 para. 3 DORA	By way of derogation from point (e), the ICT third-party service provider and the financial undertaking that is a microenterprise may agree that the access, inspection and audit rights of the financial undertaking may be transferred to an independent third party designated by the ICT third-party service provider and that the financial undertaking may at any time request information and assurance from that third party in relation to the ICT third-party service provider's access, inspection and audit rights. performance of the ICT third-party service provider.	X

[15] For further optional contractual content, see also Art. 26 para. 4 DORA.

Topic	Contract content	Reference	Extract from the legal text	kwF[13]
Inspection rights	Information access, inspection, audit and ICT testing rights	Art. 8 para. 2 RTS TPPol	The policy shall specify that the relevant contractual arrangements are to include the right for the financial entity to access information, to carry out inspections and audits, and to perform tests on ICT. For that purpose, the policy shall require that the financial entity uses the following methods, without prejudice to the ultimate responsibility of the financial entity:	X
Inspection rights	Audit by Internal Audit or an authorised third party	Art. 8 para. 2 lit. a RTS TPPol	its own internal audit or an audit by an appointed third party;	X
Inspection rights	Pooled audit and tests, incl. TLPT	Art. 8 para. 2 lit. b RTS TPPol	where appropriate, pooled audits and pooled ICT testing, including threat-led penetration testing, that are organised jointly with other contracting financial entities or firms that use ICT services of the same ICT third-party service provider and that are performed by those contracting financial entities or firms or by a third party appointed by them;	X
Inspection rights	Third-party certifications	Art. 8 para. 2 lit. c RTS TPPol	where appropriate, third-party certifications;	X
Inspection rights	Audit by the internal audit department of the third-party ICT service provider	Art. 8 para. 2 lit. d RTS TPPol	where appropriate, internal or third-party audit reports made available by the ICT third-party service provider.	X
Inspection rights	Extension of the scope of testing/certification when using certifications or test reports provided by the service provider	Art. 8 para. 3 lit. g RTS TPPol	has the contractual right to request, with a frequency that is reasonable and legitimate from a risk management perspective, modifications of the scope of the certifications or audit reports to other relevant systems and controls;	X
Inspection rights	Maintenance of audit rights for Use of certifications or audit reports provided by the service provider	Art. 8 para. 3 lit. h RTS TPPol	has the contractual right to perform individual and pooled audits at its discretion with regard to the contractual arrangements and execute those rights in line with the agreed frequency.	X
Exit	Exit strategy to ensure the continuous provision of functions	Art. 30 para. 3 lit. f number i DORA	where the third-party ICT service provider continues to provide the relevant functions or ICT services to reduce the risk of disruption to the financial undertaking or to ensure its orderly wind-down and reorganisation	X

Topic	Contract content	Reference	Extract from the legal text	kwF[13]
Exit	Exit strategy with adequate switching options	Art. 30 para. 3 lit. f number ii DORA	which enables the financial organisation to switch to another third-party ICT service provider or to switch to internal solutions, that correspond to the complexity of the service provided.	X
Exit	Exit strategies and definition of a binding, appropriate transition period	Art. 30 para. 3 lit. f DORA	Exit strategies, in particular the definition of a binding, appropriate transition period,	X
Supervision	Cooperation with competent authorities	Art. 3 para. 8 lit. c RTS TPPol	The policy shall explicitly specify that the contractual arrangements: [...] are to require that the ICT third party service providers cooperate with the competent authorities;	X
Data access	Access to data and premises	Art. 3 para. 8 lit. d RTS TPPol	The policy shall explicitly specify that the contractual arrangements: [...] are to require that the financial entity, its auditors, and competent authorities have effective access to data and premises relating to the use of ICT services supporting critical or important functions.	X
Other relevant contract contents	Specification of the relevant contractual content in accordance with the requirements of Art. 1 para. 1 lit. a DORA and other relevant laws	Art. 8 para. 1 RTS TPPol	The policy shall specify that the relevant contractual arrangement are to be in written form and are to include all the elements referred to in Article 30(2) and (3) of Regulation (EU) 2022/2554. The policy shall also include elements regarding requirements referred to in Article 1(1), point (a), of Regulation (EU) 2022/2554, as well as other relevant Union and national law as appropriate.	X
Other relevant contractual content - risk management	ICT risk management	Art. 1 para. 1 lit. a point i DORA	[Any applicable requirements in relation to] risk management in the area of information and communication technology (ICT);	X
Other relevant Contract contents - ICT incident	Reporting on important ICT-related incidents	Art. 1 para. 1 lit. a point ii DORA	[Any applicable requirements in relation to] reporting of serious ICT-related incidents and - on a voluntary basis - significant cyber threats to the relevant authorities;	X
Other relevant contractual content - ICT incident	Reporting on important payment transactions	Art. 1 para. 1 lit. a point iii DORA	[Any applicable requirements in relation to] reporting of serious payment-related operational or security incidents by financial entities listed in Article 2(1)(a) to (d) to the competent authorities;	X
Other relevant contract contents - DOR tests	DOR tests	Art. 1 para. 1 lit. a point iv DORA	[Any applicable requirements in relation to] digital operational resilience testing;	X

Topic	Contract content	Reference	Extract from the legal text	kwF[13]
Other relevant contractual content - exchange of cyber Information on	Exchange of cyber information	Art. 1 para. 1 lit. a point v DORA	[Any applicable requirements relating to] sharing information and intelligence relating to cyber threats and vulnerabilities;	X
Other relevant contractual content - risk management	Third-party risk management	Art. 1 para. 1 lit. a point vi DORA	[Requirements, if any, in relation to] measures for the sound management of third party ICT risk;	X
Monitoring	Measures and key indicators for monitoring performance, information security requirements and the financial organisation's policies and processes	Art. 9 para. 1 RTS TPPol	The policy shall require that the contractual arrangements specify the measures and key indicators to monitor, on an ongoing basis, the performance of ICT third party service providers, including measures to monitor compliance with requirements regarding the confidentiality, availability, integrity and authenticity of data and information, and the compliance of the ICT third-party service providers with the financial and legal requirements. entity's relevant policies and procedures. […]	X
Monitoring	Measures for inadequate service quality	Art. 9 para. 1 RTS TPPol	[...] The policy shall also specify measures that apply when service level agreements are not met, including contractual penalties where appropriate.	X
Cancellation	Securing contractual cancellation rights	Art. 28 para. 7 DORA	Financial companies ensure that contractual agreements on the use of ICT services can be cancelled if one of the following circumstances occurs:	
Cancellation	Right of cancellation in the event of a significant breach of existing regulations	Art. 28 para. 7 lit. a DORA	a significant breach by the ICT third-party service provider of applicable laws, other regulations or contractual conditions;	
Cancellation	Right of cancellation if adverse circumstances are identified	Art. 28 para. 7 lit. b DORA	Circumstances identified in the course of monitoring the ICT third party risk that are assessed as likely to affect the performance of the functions provided for under the contractual arrangement, including material changes affecting the arrangement or the circumstances of the third party. ICT third-party service provider;	

Cancellation	Right of termination in the event of evidence of weaknesses in the ICT risk management of the ICT third-party service provider	Art. 28 para. 7 lit. c DORA	demonstrable weaknesses of the third-party ICT service provider in its overall ICT risk management and in particular in the way it ensures the availability, authenticity, security and confidentiality of data, whether personal or otherwise sensitive data or non-personal data;

Topic	Contract content	Reference	Extract from the legal text	kwF[13]
Cancellation	Right of cancellation in circumstances that prevent effective supervision by the competent authority	Art. 28 para. 7 lit. d DORA	the competent authority can no longer effectively recognise the financial undertaking as a result of the terms of the relevant contractual agreement or the circumstances associated with that agreement supervise.	
Subcontracting - cancellation	Cancellation rights in connection with subcontracting	Art. 7 para. 1 RTS-E SUB	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:	X
Subcontracting - cancellation	Right of cancellation in the event of uncoordinated, significant changes to subcontracting	Art. 7 para. 1 lit. a RTS-E SUB	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,	X
Subcontracting - cancellation	Right of termination in the event of explicitly unauthorised subcontracting of critical or important functions	Art. 7 para. 1 lit. b RTS-E SUB	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.	X
Subcontracting	Obligation to reproduce the relevant contract contents in the case of subcontracting	Art. 3 para. 1 lit. c RTS-E SUB	that the relevant clauses of the contractual arrangements between the financial entity and the ICT third-party service provider are replicated as appropriate in the subcontracting arrangements between the ICT third-party service provider and its subcontractor to ensure that the financial entity is able to comply with its own obligations under Regulation (EU) 2022/2554;	X
Subcontracting	Description and conditions under which subcontracting is permitted	Art. 4 RTS-E SUB	When describing in the written contractual arrangements the ICT services to be provided by an ICT third-party service provider in accordance with Article 30(2)(a) of Regulation (EU) 2022/2554, financial entities shall identify which ICT services support critical or important functions and which of those are eligible for subcontracting and under which conditions. 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:	X
Subcontracting - Monitoring	Monitoring obligations with regard to the subcontracting of critical or important functions	Art. 4 lit. a RTS-E SUB	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;	X

Topic	Contract content	Reference	Extract from the legal text	kwF[13]
Subcontracting - monitoring and Reporting obligations	Monitoring and reporting obligations vis-à-vis the financial undertaking	Art. 4 lit. b RTS-E SUB	the monitoring and reporting obligations of the ICT third-party service provider towards the financial entity;	X
Subcontracting - Risk assessment	Assessment of all risks (incl. location-related ICT risks)	Art. 4 lit. c RTS-E SUB	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;	X
Subcontracting - Location	Data processing and storage location of subcontracted ICT services	Art. 4 lit. d RTS-E SUB	the location and ownership of data processed or stored by the subcontractor, where relevant;	X
Subcontracting - monitoring and reporting obligations	Description of the subcontractor's monitoring and reporting obligations	Art. 4 lit. e RTS-E SUB	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;	X
Subcontracting - Business continuation management	Commitment to continuous service provision	Art. 4 lit. f RTS-E SUB	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;	X
Subcontracting - Business continuation management	Business continuation management at the subcontractor	Art. 4 lit. g RTS-E SUB	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;	X
Subcontracting - Security	ICT security standards at the subcontractor	Art. 4 lit. h RTS-E SUB	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;	X
Subcontracting - inspection rights & data access	Granting of comparable audit, information and access rights	Art. 4 lit. i RTS-E SUB	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 entity and relevant competent authorities by the ICT third-party service provider;	X
Subcontracting - cancellation	Cancellation rights in the event of adverse circumstances	Art. 4 lit. j RTS-E SUB	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;	X

Topic	Contract content	Reference	Extract from the legal text	kwF[13]
Subcontracting - notification period	Sufficient notification period for significant changes in subcontracting and obligation not to implement any changes within this period, as well as the right to demand changes	Art. 6 para. 1 RTS-E SUB	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.	X
Subcontracting - right of objection	No changes to the subcontract award during the notification period or without consent	Art. 6 para. 3 RTS-E SUB	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.	X
Subcontracting - right of objection	Right to request adjustments to planned changes to subcontracting	Art. 6 para. 4 RTS-E SUB	The financial entity shall have a right to request modifications to the proposed subcontracting changes before their implementation if the risk assessment referred to in paragraph 1) concludes that the planned subcontracting or changes to 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.	X