BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

Supervisory notice

Information on the implementation of DORA in ICT risk management and ICT third party risk management

Banking supervision
IT Supervision and Supervisory Support Policy Unit

Status: June 2024

Table of contents

I. Foreword

With DORA (Digital Operational Resilience Act), Regulation (EU) 2022/2554 on digital operational resilience in the financial sector, the European Union has established a European regulation for digital operational resilience across the financial sector,
ICT risks and cyber security. The regulation came into force on 16 January 2023 and will apply from 17 January 2025. From this date, the requirements of DORA must be fulfilled by all financial companies.

ICT risk management is the overarching core element of DORA. It is intended to provide financial organisations with a framework with which they can systematically identify, assess and manage their ICT risks. The requirements for ICT risk management therefore basically cover the topics addressed by BaFin via the supervisory requirements for IT (BAIT/VAIT/KAIT/ZAIT). Nevertheless, the methodological approach of the regulations differs, which can lead to challenges when implementing the DORA requirements.

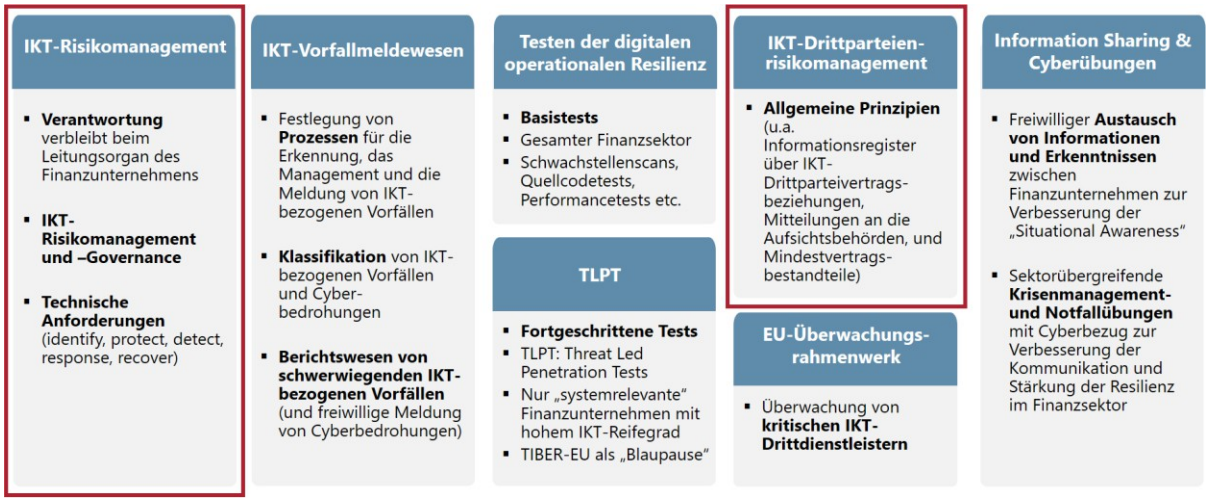
This supervisory communication is intended to provide support in the implementation of the DORA requirements for ICT risk management (Chapter II) and ICT third-party risk management (Chapter V Section I), including the relevant regulatory technical standards (RTS)[1] . It is aimed in particular at those companies supervised by BaFin that fall under the scope of application of the Banking Supervision Requirements for IT (BAIT) or the Insurance Supervision Requirements for IT (VAIT) and will in future have to comply with the requirements for ICT risk management in accordance with Art. 5 to 15 DORA, among others. Even if these implementation instructions only relate to BAIT/VAIT, the supervisory requirements for capital management companies and payment and e-money institutions (KAIT/ZAIT), which are not explicitly considered here, are comparable in many cases, meaning that the results can generally be transferred.

The implementation guidelines are based on the results of six working groups set up in 2023, which were made up of representatives from industry, the Deutsche Bundesbank and BaFin. The working groups compared the DORA requirements for the aforementioned "regular ICT risk management framework" and the "key principles for sound management of third party ICT risk" (Art. 28 - 30 DORA) and the associated draft RTS with the requirements of Chapters 1 to 10 BAIT and VAIT in order to identify significant changes and any resulting need for action[2] . The other chapters of DORA were not considered in this context (see Figure 1).

[1] The Level 2 texts must always be considered together with DORA. The final versions are published by the European Commission in the Official Journal of the EU.

[2] The requirements for the simplified ICT risk management framework (Art. 16 DORA) require separate consideration and are not part of this analysis.

Figure 1: Key elements in DORA



The implementation instructions take into account the current status of the following RTS or draft RTS (Level 2 legal texts) at the time of publication:

- COMMISSION DELEGATED REGULATION (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework (hereinafter "RTS RMF")
- 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 (hereinafter "RTS TPPol")
- Consultation Paper on 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 (hereinafter "RTS-E SUB")

Subsequent amendments to the RTS-E SUB cannot be ruled out due to the ongoing European legislative process, which ends with the publication of the legal text in the Official Journal of the European Union.

The principle of proportionality is not explicitly stated in the implementation instructions. This is standardised in Art. 4 DORA for Chapters II, III and IV. This ensures that financial companies can take a risk-based approach when applying DORA. The exemptions for micro-enterprises contained in the individual articles are also not explained.

Similarly, the definitions in Art. 3 DORA are only referred to in the analysis where relevant. Neither the BAIT nor the VAIT contain a comparable list of defined key terms.

The Implementation Guidance does not constitute a binding interpretation by BaFin, nor does it constitute an interpretation within the framework of the question and answer processes (Q&As) of the three European supervisory authorities (EBA - European Banking Authority, ESMA - European Securities and Markets Authority and EIOPA - European Insurance and Occupational Pensions Authority).

In this publication, BaFin has used some of its own translations of the English-language drafts of the Level 2 legal texts, as these were the basis for the discussions. The original English texts are authoritative.

II. Implementation instructions

The following implementation instructions for implementing the requirements of DORA are divided into the sections Governance and Organisation, Information Risk and Information Security Management, IT Operations, ICT Business Continuity Management,
IT Project Management and Application Development, ICT Third Party Risk Management, Operational Information Security and Identity and Rights Management.

Overall, it should be noted that the requirements of BAIT and VAIT are essentially reflected in the requirements of DORA for the "regular ICT risk management framework".
(Art. 5 - 15 DORA) and the "Key principles for sound management of third party ICT risk" (Art. 28 - 30 DORA) as well as the relevant Level 2 legal texts or their drafts. Due to its focus on digital operational resilience, DORA also contains requirements that are not yet reflected in the BAIT/VAIT.

In light of this assessment and the national implementation of DORA through the Financial Market Digitalisation Act (FinmadiG), BaFin intends to repeal the supervisory requirements for IT (BAIT/VAIT/KAIT/ZAIT). For financial companies that do not fall under the scope of DORA, it should be noted that measures for the appropriate handling of IT/cyber risks must be taken in any case as part of the proper business organisation.

1. Governance and organisation

This section sets out the requirements of Art. 5 and 6 DORA and Art. 2
(2) RTS RMF on the governance and organisation of ICT risk management in DORA are compared with those in the IT strategy (Chapter 1) and IT governance (Chapter 2) chapters of BAIT/VAIT.

An IT strategy, as required in Chapter 1 BAIT/VAIT, is not specified in DORA. DORA, on the other hand, contains requirements for the strategy for digital operational resilience (hereinafter referred to as the DOR strategy). As the two strategies consider different aspects, some of the requirements for the DOR strategy are new.

DORA focuses on the governance and organisation of ICT risk management, i.e. the effective and prudent management of ICT risks to strengthen the digital resilience of the individual financial company through an internal governance and control framework. In contrast, information security and the associated governance requirements are at the centre of the requirements in BAIT/VAIT. The differences can also be seen in the content of the new DOR strategy as the central strategy of the ICT risk management framework or in the extended tasks of the management body.

DORA also refers in Art. 6 para. 8 lit. g DORA to extensive additional requirements for testing digital operational resilience (see Chapter IV, Art. 24 - 27 DORA). The results of the tests described in the requirements should serve, among other things, to

mitigate ICT risks and achieve specific ICT objectives. However, these additional requirements in Chapter IV are not the subject of these implementation guidelines.

1.1 DORA calls for new strategy for digital operational resilience

DORA introduces a new DOR strategy (Art. 6 para. 8 DORA). This strategy focuses on ICT risk management, which also includes ICT third party risk management. In comparison, the BAIT/VAIT set requirements for the IT strategy, i.e. the functional, overarching and significantly broader strategy for the entire IT. These differences are also evident in the minimum requirements for the content of the two strategies, meaning that the two strategies cannot be equated. Certain content that BAIT/VAIT require in the IT strategy can be found in DORA as part of the general, non-strategy-related requirements. These are then usually part of the requirements from ICT governance. For example, the strategic development of the IT organisational structure and IT process organisation (Chapter 1.2 lit. a BAIT/VAIT) is mapped in DORA as requirements for the organisation of ICT below the strategy level (Art. 5 Para. 2 and Art. 6 Para. 5 DORA). Statements on IT emergency management, as listed in the IT strategy, are not explicitly included in the DOR strategy. However, the topic of ICT business continuity management is a requirement of the ICT risk management framework (see section 4) and is one of the tasks of the governing body (see section 1.3).

The allocation of common standards (section 1.2 lit. b BAIT/VAIT) to the implementation of information security requirements from the IT strategy is also not reflected in the DOR strategy. However, DORA also suggests, much less prominently, the consideration of common standards (Art. 2 para. 2 lit. h RTS RMF) and also remains standard-neutral in its requirements and their implementation by financial institutions.

With regard to the objectives, responsibilities and integration of information security into the organisation (section 1.2 lit. c BAIT/VAIT), corresponding requirements can also be found in the DOR strategy. The DOR strategy sets out clear, verifiable information security objectives. With regard to relationships with ICT third party risks, the ICT third party risk strategy in accordance with Art. 28 para. 2 DORA and the optional strategy for the use of multiple ICT providers in Art. 6 para. 9 DORA must be observed. In contrast, the embedding of information security in the specialist areas is reflected in DORA at the level of the respective guidelines for ICT security.

The strategic development of the IT architecture (Chapter 1.2 lit. d BAIT/VAIT) is comparable to the requirements of the DOR strategy in Art. 6 para. 8 DORA for the ICT reference architecture, including an explanation of any changes that are necessary to achieve specific business objectives. However, the term ICT reference architecture is newly introduced in DORA and is not defined in Art. 3 DORA, so that in the demarcation, the term "ICT reference architecture" may not be used.
blurring can occur.

In contrast to the VAIT, DORA makes no statement regarding the form of the document - separately or as part of the business strategy - but it can still be assumed that strategies can be combined appropriately. With regard to the appropriate

Communication of the IT strategy (Chapter 1.5 VAIT) has no equivalent in DORA, although general sectoral governance requirements must be observed here.

Even if DORA does not require an IT strategy in the sense of BAIT/VAIT, its continued existence is absolutely necessary and sensible, both as a possible link between business strategy and DOR strategy and against the background of sectoral requirements for strategies in the business organisation.

1.2 Comprehensive but ICT-specific internal governance and control framework

The internal ICT governance framework and control framework is a focal point in DORA. It should be noted that the general, non-ICT-specific governance requirements from the sectoral regulations remain in place. DORA addresses the governance of the ICT risk management framework, i.e. the effective and prudent management of ICT risks and, as a result, the strengthening of the resilience of the respective financial organisation. In BAIT/VAIT, the focus is somewhat different and is particularly focussed on information security and the associated governance requirements.

DORA also requires an overall view of risk, as ICT risk management is included in the general risk management of financial companies (Art. 6 para. 1 DORA). Like BAIT/VAIT (see preliminary remarks in section 4.2 VAIT, section 4.2 BAIT/VAIT), DORA emphasises the ultimate and overall responsibility of the management body in this context (Art. 5 para. 2 lit. a, d DORA).

With regard to the establishment of an ICT risk control function with responsibility for the management and monitoring of ICT risks in accordance with Art. 6 (4) DORA (see section 2.2), DORA requires appropriate separation and independence from the various functions. The BAIT/VAIT generally require the avoidance of conflicts of interest and incompatible activities in the IT structure and IT process organisation (section 2.4/ 2.7 BAIT/VAIT). DORA requires the three lines of defence model or the use of other internal models for risk management and control (Art. 6 para. 4 DORA).

In addition to the ICT risk control function, DORA provides for the establishment of a monitoring function in Art. 5 Para. 3, which includes contracts with third-party ICT service providers for the use of ICT services.
ICT services. It is to be performed either by a function to be set up or by a member of management (see also section 6.6).

The general requirements for the guidelines for ICT security prescribed in Art. 2 Para. 2 RTS RMF do not exist in the BAIT/VAIT. However, there are overlaps in terms of content/context between the individual guidelines for ICT security and the BAIT/VAIT. Due to the differences, adjustments may be necessary on the part of financial organisations.

The consideration of the state of the art and the future threat situation (Chapter 2.3/2.4 BAIT/VAIT) are also present in DORA, albeit under different terminology (cf. inter alia recital 48 DORA and Art. 2 para. 2 RTS RMF).

1.3 Significant expansion of the tasks of the management body

DORA assigns significantly more responsibility to the management body through detailed requirements and tasks (Art. 5 para. 2 DORA) and thus strengthens its role in the context of governance and organisation. Similar requirements can be found in the BAIT/VAIT as a task of the management at specific points (including IT strategy, regulations on IT structure and IT process organisation, control of IT operations, IRM, information security guideline, ISM, investigation of information security incidents, IT project management), but are less extensive.

Art. 5 para. 4 DORA requires the members of the management body to have sufficient knowledge and skills regarding the ICT risks to be managed, which must be actively kept up to date. There is no explicit equivalent to this in the BAIT/VAIT; rather, the circulars generally require adequate quantitative and qualitative resources.

In many cases, the management body of the financial company is responsible for defining, authorising, monitoring and taking responsibility for arrangements in connection with the ICT risk management framework (cf. in particular Art. 6 para. 1 DORA):

- According to Art. 5 para. 2 lit. b DORA, guidelines for maintaining high standards in relation to the four protection objectives of DORA are to be introduced, including the information security guideline of Art. 9 para. 4 lit. a DORA, the guideline on the
  ICT business continuation management and ICT third party risk management.
- The guidelines for ICT security listed in the RTS RMF must also be approved by the management body (Art. 2 para. 2 lit. b RTS RMF). The BAIT/VAIT do not recognise a comparable requirement at the level of guidelines.
- The avoidance of conflicts of interest through suitable organisational measures prescribed in Chapter 2.4/2.7 BAIT/VAIT is also a subject of the requirements in DORA. Although the "avoidance of conflicts of interest" is not explicitly mentioned in DORA, it results from the governance requirements and is also listed in particular in Art. 2 para. 2 lit. g RTS RMF. The task of defining clear tasks and responsibilities for all ICT-related functions are the responsibility of the management body in accordance with Art. 5 para. 2 lit c DORA.
- The implementation of the ICT business continuity policy and the ICT response and recovery plans must be regularly approved, monitored and reviewed.
- Like BAIT/VAIT, DORA also stipulates an appropriate level of resources to meet the requirements for digital operational resilience; this also includes ICT skills for all employees. Ensuring this is the responsibility of the management body (Art. 5 para. 2 lit. g DORA).
- The internal ICT audit plans of the ICT audit and significant changes to these must be regularly approved and reviewed.

2. Information risk and information security management

This section compares the requirements for information risk and information security management and the ICT risk management framework of Art. 3, 5, 6, 8, 13, 14, 45, 49 DORA and Art. 3 - 5 and 27 RTS RMF with those of the chapters on information risk management and information security management of BAIT/VAIT.

ICT risk management is of central importance for DORA in order to achieve the goal of digital operational resilience. Compared to BAIT/VAIT, DORA places a much stronger emphasis on ICT risk management than on information security. This is also reflected in the introduction of the ICT risk control function, which is intended to assume "responsibility for the management and monitoring of ICT risk". It is similar to the Information Security Officer (ISO) known from BAIT/VAIT - who is, however, more responsible for information security issues.

Furthermore, new auditing and analysis requirements for ICT risks, new technologies, legacy systems, incidents and tests have been introduced, as well as associated reporting obligations, including to the supervisory authority. For example, a review of the ICT risk management framework is planned at least once a year or on an ad hoc basis, which can be requested by the supervisory authority in the form of a report. DORA also emphasises training obligations and communication strategies against the backdrop of digital operational resilience.

2.1 Shift in emphasis from information security to ICT risk management

There is a fundamental shift in emphasis due to the much stronger emphasis on ICT risk management compared to information security. According to DORA, the
ICT risk management is the basis for ensuring digital operational resilience, for which information security measures are used. In the BAIT/VAIT, the focus is on information security measures, followed by the risk assessment. However, the measures actually required in practice are unlikely to differ significantly between the two approaches. A stronger focus on the
ICT risk on the basis of this shift in emphasis, with a corresponding prioritisation in implementation, is, however, entirely conceivable.

Furthermore, DORA does not prohibit the outsourcing[3] of ICT risk management functions. Art. 6 para. 10 DORA explicitly refers to the outsourcing of the "verification of compliance with ICT risk management requirements". In the event of outsourcing, however, sector-specific requirements[4] regarding outsourcing must still be observed. In the specific case of outsourcing, these sectoral regulations may well define prerequisites, conditions or limits for such outsourcing. The financial company also remains fully responsible for ensuring ICT risk management.

[3] This includes spin-offs.
[4] For example, Circular 05/2023 (BA) - Minimum requirements for risk management (MaRisk), Circular 2/2017 (VA) - Minimum requirements for the business organisation of insurance companies (MaGo) or guidelines from the European supervisory authorities on outsourcing.

The definition of an information network in accordance with Chapter 3.3/3.4 BAIT/VAIT and the procedure for determining protection requirements in accordance with Chapter 3.4/3.5 BAIT/VAIT are replaced by ICT asset management and the classification of these assets. DORA focuses on the determination or identification and classification of ICT-supported business functions as well as information assets and ICT assets that support these functions (Art. 8 para. 1 DORA and Art. 4 and 5 RTS RMF). Critical assets as well as dependencies on third-party ICT service providers and risks from cyber threats and
Identify ICT vulnerabilities. The documentation should take place in inventories. The obligation to record the configuration of information assets and ICT assets and the connections/interdependencies between the assets also creates a content-related proximity to a configuration management database (CMDB). If the
If it is ensured that the DORA specifics are covered, the procedures for defining the information network can be used in conjunction with the requirement to manage components of the IT systems from IT operations and the determination of protection requirements for implementation; however, other possible solutions are also conceivable.

2.2 Greater focus on analysis and control activities

DORA introduces an ICT risk control function in Art. 6 Para. 4 DORA, which corresponds to the risk control function described in
Chapter 4.4/4.5 BAIT/VAIT is very similar to the position and independence of the Information Security Officer (ISB), but is not identical. For example, the ISB is to be responsible for the "management of all information security matters", while the control function is to assume "responsibility for the management and monitoring of ICT risk". The further development of the ISB into an ICT risk control function seems sensible in order to take this change into account. If the aim is for the ICT risk control function to be taken over by the ITS, it should be ensured that it also fulfils the tasks of ICT risk management. The less detailed definition of the specific tasks of the ICT risk control function also opens up room for manoeuvre for a modified task structure.

DORA prescribes extensive new auditing and analysis requirements for ICT risks, new technologies, legacy systems, incidents and tests, as well as associated reporting obligations, in some cases also to the supervisory authority. These include in particular

- A review of the ICT risk management framework in accordance with Art. 6 para. 5 DORA should be carried out at least once a year or on an ad hoc basis if serious risks arise.
  ICT-related incidents or findings from tests (Chapter IV DORA) or audits. Continuous improvement of the ICT risk management framework builds on this. The supervisory authority can request a review and request a report on the review (Title II, Chapter V RTS RMF).
- Following serious ICT-related incidents that disrupt core activities, the cause of the incident must be investigated and necessary improvements identified (Art. 13 para. 2 DORA). The speed of response, any forensic analyses, escalation and communication must also be addressed.
- The specific risks for all legacy ICT systems must be assessed at least annually (Art. 8 para. 7 in conjunction with Art. 3 no. 3 DORA). This risk assessment must "in any case

before and after the connection of technologies, applications or systems".

- Senior ICT staff should report to the governing body at least annually on findings from incidents and tests and submit their recommendations (Art. 13 para. 5 DORA). This relates in particular to cyberattacks and other emergency-related incidents, as well as threat-led penetration testing (TLPT) or supervisory reviews.

It can be assumed that new processes will have to be created or existing ones adapted in order to implement these analysis and reporting obligations. In addition to the retrospective look at ICT-related incidents and the performance of the ICT risk management framework in the past, new technological developments, including with regard to cyber attacks, should also be monitored (Art. 13 para. 7 DORA and Art. 3 para. 1 lit. e RTS RMF). The aim is to analyse the impact of the use of new technologies on ICT security and digital operational resilience. One focus is on observing the "latest" ICT risk management processes for effective defence against existing and new forms of cyber attacks.

2.3 Strengthening training and communication

DORA emphasises training obligations much more strongly than BAIT/VAIT. For example, financial institutions must develop ICT security awareness programmes and digital operational resilience training for their employees and management (Art. 13 para. 6 DORA). In addition, the members of the management body are required to keep their ICT risk skills up to date, including through specialised training (Art. 5 para. 4 DORA). In general, the training should be tailored to the area of responsibility and also cover any third-party ICT service providers used.

As part of the ICT risk management framework, financial organisations must establish communication strategies[5] , guidelines and plans at least for serious ICT incidents and vulnerabilities in order to enable responsible disclosure of incidents and vulnerabilities (Art. 14 DORA). A distinction should be made between the different addressees - including explicitly the public. Financial organisations must appoint at least one person to implement the communication strategy for ICT-related incidents, who will perform the corresponding task vis-à-vis the public and the media for this purpose (Art. 14 para. 3 DORA).

Financial companies can voluntarily participate in an information exchange on cyber threats and information within trusted communities (Art. 45 para. 1 DORA). Participation in such an information exchange must be reported to the supervisory authority, as must the termination of the cooperation.

[5] In the German language version of DORA, the translation from English in Art. 14 para. 2 DORA is, in our opinion, incorrect: the English term "communication policies" should be translated as "Kommunikationsleitlinien" instead of "Kommunikationsleitlinien".
"communication strategies".

(Art. 45 para. 3 DORA). In accordance with Art. 49 (1) DORA, supervisory authorities can offer crisis management and emergency exercises in order to practise a coordinated response and develop communication channels.

3. IT operations

In this section, the provisions of Art. 7, 8, 9 and 12 DORA as well as the Art. 4, 5, 8, 9 and 17 RTS RMF on the operation of IT systems are compared with Chapter 8 IT operations of BAIT/VAIT.

IT operations are becoming increasingly important in the context of strengthening digital operational resilience. Requirements for up-to-date, reliable and technologically resilient ICT systems are included in DORA to a greater extent than before. The detailed overview of the ICT systems is also more closely interlinked with the business functions. As a result, ICT systems, information and their interactions with each other are now jointly identified, classified and managed in the form of an inventory. In addition, more changes to these systems than before must be considered as part of change management. The backup and restoration of data is supplemented by requirements such as separate systems or multiple checks after a restore.

3.1 Increased operational stability

In the context of digital operational resilience, a further focus is on the operational stability and updating of ICT systems. Art. 7 DORA emphasises this and thus tightens the existing requirements of BAIT/VAIT. For example, Art. 7 DORA requires "ICT systems to be kept up to date at all times" and thus goes beyond the previous regulation, which primarily required IT systems to be updated (section 8.3 BAIT/VAIT). Furthermore, the requirements for the reliability (Art. 7 lit. b DORA) and technological resilience (Art. 7 lit. d DORA) of ICT systems have been expanded. ICT systems must ensure appropriate information processing even in tense market phases. These requirements were not previously emphasised so explicitly in BAIT/VAIT.

The capacity management known from section 8.8 BAIT/VAIT is also supported by Art. 7 lit. c DORA in conjunction with Art. 9 RTS RMF. For example, this must be documented to a greater extent than before. In addition, measures for resource optimisation must be determined and resource bottlenecks must be analysed and averted before they occur through appropriate monitoring. Redundant ICT capacities with resources, capabilities and functions that are sufficient and appropriate to cover business needs are also required in Art. 12 para. 4 DORA.

In the course of strengthening resilience, the review of existing legacy ICT systems will also become more important than before. These already had to be managed (Chapter 8.3 BAIT/VAIT), but in future they must be explicitly analysed once a year and whenever the ICT risk changes and assessed with regard to the ICT risk they pose (Art. 8 para. 7 DORA).

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).

The procedures for securing and restoring are in accordance with Art. 12 para. 2 DORA and 8.7 BAIT/VAIT must be tested regularly. When restoring data, it should be noted that Art. 12 para. 3 DORA stipulates ICT systems that are physically and logically separated from the source system. This is only listed as a possible requirement in BAIT/VAIT. DORA therefore exceeds the previous requirements of BAIT/VAIT with regard to data storage.

In addition, Art. 12 para. 7 DORA introduces checks of data during data recovery after ICT-related incidents, which also include multiple checks and reconciliations to ensure the greatest possible data integrity. The BAIT/VAIT do not provide for such a form of data reconciliation or verification.

The reporting of unplanned deviations from normal operation (disruptions) is already known from chapter 8.6 BAIT/VAIT. DORA uses the term "incident" for these disruptions. "errors" or faults (Art. 8 para. 2 lit. c RTS RMF). Similar to faults, these errors must continue to be analysed using suitable procedures and protocols.

In addition, DORA refers to extensive additional requirements within ICT risk management for the treatment, classification and reporting of
ICT-related incidents (see Chapter III, Art. 17 - 23 DORA) and testing (see Chapter IV, Art. 24 - 27 DORA). However, Chapters III and IV DORA are not the subject of these implementation instructions.

4. ICT business continuation management

In this section, the relevant requirements of Art. 11, 12 and 14 DORA and Art. 24 to 26 RTS RMF for ICT business continuity management and response and recovery (hereinafter referred to as ICT business continuity management) are assigned to the chapters
IT operations and (IT) emergency management of BAIT/VAIT (Chapter 10 in each case).

To summarise, it should be noted that Art. 11 DORA and Art. 24 to 26 RTS RMF are broader than the requirements listed in Chapter 10 BAIT/VAIT. Significant differences result from changes in the content and structure of the relevant guidelines and plans, which centre on the ICT Business Continuity Guideline.

In addition, the number of scenarios to be considered has increased compared to the BAIT/VAIT: For example, the effects of climate change and insider attacks in particular must be included in the development of ICT response and recovery plans.

Further changes arise in the review of ICT business continuity management, which in DORA is the responsibility of the management body with regard to the ICT business continuity policy and the ICT response and recovery plans and is not specified in BAIT/VAIT. DORA provides for regular or at least annual intervals for the review and testing of the various ICT business continuity management plans and thus differs from BAIT/VAIT. In addition, DORA significantly tightens these requirements compared to BAIT/VAIT by establishing a crisis management function and a stronger overall focus on (crisis) communication.

In addition, DORA provides for reporting on request to the competent authorities on the estimated aggregate annual costs and losses caused by serious ICT-related incidents. Details are specified in a guideline. This report is not part of these implementation instructions.

4.1 Changed structure and content of guidelines and plans

As a central element of ICT business continuation management in accordance with Art. 11 (1) DORA, which is an integral part of the general business continuity guideline and is based on the identification requirements of Art. 8 DORA (see section 2.2). The term ICT Business Continuity Guideline is not used in the BAIT/VAIT. BAIT/VAIT use the term business continuity plans in the chapter on IT operations and in the introduction to the chapter on IT emergency management (BAIT).

The objectives of the ICT Business Continuity Guideline are listed in Art. 11 para. 2 DORA. In addition to the requirement for documentation, this guideline includes in particular

- the appropriate response to all ICT-related incidents to limit damage, combined with the resumption of activities and the prioritisation of recovery measures;
- the activation of plans with containment measures, processes and technologies in the event of ICT-related incidents, and
- the mandatory assessment of preliminary impacts, damages and losses (as may already be implemented in the context of PSD2 notifications of serious operational and security incidents);
- the definition of communication and crisis management measures.

The components of the ICT Business Continuity Guideline are described in detail in Art. 24 RTS RMF. A business impact analysis (BIA) and risk analysis must be taken into account for serious business disruptions when implementing the general business continuity guideline, whereby the risk analysis in DORA is part of the BIA (Art. 11 para. 5 DORA and chapters 10.3, 10.4 VAIT). The corresponding framework conditions must be listed in the business continuation guideline.

When determining the recovery time and recovery points for each function, financial institutions take into account not only the critical or important function but also the potential overall impact on market efficiency (Art. 12 para. 6 DORA and Chapter 10.3/10.5 BAIT/VAIT). The latter is introduced in DORA.

The business continuation plans listed in chapters 8.7, 10.1/ 8.7 BAIT/VAIT are not included in DORA. With the ICT business continuation plans (Art. 11 para. 4 DORA), DORA contains a comparable construct. These plans must be regularly maintained (Art. 11 para. 4 DORA) and tested (see section 4.3). Art. 25 RTS RMF prescribes further requirements for the testing of ICT business continuity plans. Accordingly, outsourcing and contractual agreements with third-party ICT service providers must be included in the creation, maintenance and testing of business continuity plans, particularly with regard to critical and important functions (Art. 25

Para. 2 RTS RMF). The results of the above-mentioned BIA and the ICT risk assessment must be taken into account (Art. 3 para. 1 lit. b DORA).

The term "IT contingency plans" relating to the restart, emergency operation and recovery plans (see in particular Chapter 10.3/10.5 BAIT/VAIT) is not found in DORA. DORA introduces ICT response and recovery plans at this level (Art. 11 para. 3 DORA). These plans are further specified in Art. 26 RTS RMF.

Like the ICT business continuity plans, the ICT response and recovery plans must also be tested (Art. 11 para. 6 lit. a DORA, see section 4.3). Art. 11 para. 6 lit. b DORA also provides for the testing of crisis communication plans. There is no such requirement in BAIT/VAIT. The test results are published under DORA
and all deficiencies identified during the tests must be analysed, rectified and reported to the management body.

4.2 Expansion of mandatory scenarios

The mandatory consideration of specific scenarios is listed in DORA when preparing the ICT response and recovery plans (Art. 26 para. 2 RTS RMF) and is linked to the components of the ICT business continuity guideline and the general business continuity guideline (Art. 24 para. 1 lit. b point i para. 1 and
Art. 25 para. 2 lit. e RTS RMF). Furthermore, the number of scenarios to be taken into account differs from BAIT/VAIT. The following scenarios are new:

- Effects of climate change and events related to environmental degradation, natural disasters, pandemics and physical attacks, including burglaries and terrorist attacks;
- Insider attacks;
- political and social instability, including, where applicable, in the country in which the third-party ICT service provider provides its services and in the place where the data is stored and processed, and
- Large-scale power failures.

4.3 Regular review of ICT business continuation management

According to BAIT, the (IT) emergency concept must be regularly reviewed for effectiveness and appropriateness and according to VAIT, it must be regularly reviewed - including the IT emergency plans - to ensure that it is up to date.
The VAIT required the IT emergency plan to be updated on an ad hoc basis. In DORA, the management body or the financial undertaking is responsible for approving and regularly monitoring the ICT business continuity policy and the ICT response and recovery plans (Art. 5 para. 2 lit. e DORA and Art. 11 para. 6 DORA regarding the review). However, the differences in terminology must be taken into account here, meaning that a direct comparison is not possible without further ado.

There is no direct equivalent in DORA for the at least annual review of the effectiveness and appropriateness of all relevant scenarios and activities in BAIT.

The regular tests of the ICT business continuity plans provided for in Art. 11 para. 6 lit. a DORA have no direct equivalent in BAIT/VAIT. The tests of the ICT response and recovery plans, which are also required, are comparable to the requirements for annual (BAIT) or regular (VAIT) tests of the effectiveness of the
IT contingency plans, as they have an overlap with these IT contingency plans. However, these tests must be carried out at least annually and in the event of any significant changes to ICT systems that support critical or important functions (Art. 11 para. 6 lit. a DORA).

As already discussed in section 2.2, the ICT risk management framework, which includes ICT business continuity management, must be reviewed at least annually or similar.

4.4 Strengthening crisis management and communication

Art. 11 para. 7 DORA provides for the establishment of a crisis management function. W h e n activating ICT business continuity plans or ICT response and recovery plans, this should, among other things, define clear procedures for handling internal and external crisis communication (Art. 14 DORA).

Communication and crisis management measures must be put in place as part of the ICT Business Continuity Guideline and in particular i n t h e context of ICT-related incidents. These measures are aimed at informing both external stakeholders and internal employees involved (Art. 11 para. 2 lit. e in conjunction with Art. 14 and 19 DORA; Art. 24 para. 1 lit. a no. iv and lit. b no. vi RTS RMF). For implementation, communication strategies and guidelines must be developed that take into account the information needs of the employees involved in response and recovery and the other personnel to be informed (Art. 14 para. 2 DORA).

5. IT project management and application development

In this section, the requirements of Art. 15, 16, 17 RTS RMF for ICT project and change management are compared with the requirements for IT project management and change management.
-This is compared with the application development of Chapter 7 BAIT/VAIT.

Overall, it should be noted that the individual requirements with specific IT security characteristics in the RTS RMF contain significantly more details than the BAIT/VAIT in the chapter on IT projects and application development. The focus in the RTS is clearly on the Implementation of suitable measures to fulfil the security objectives and less on the governance of certain processes, as in the BAIT/VAIT. The measures listed in the RTS RMF represent minimum requirements and should not be interpreted as exhaustive. Accompanying measures to the minimum requirements can also be demanded here in accordance with the principle of proportionality.

If BAIT/VAIT is implemented, the new regulations will result in a greater degree of freedom when implementing the requirements. In DORA, fewer details and examples are given in relation to ICT project and change management. Rather, the security level is defined via minimum requirements, but implementation is left more free.

designed. Moderate additional effort is nevertheless required to check the source codes and implement the materiality threshold that has been removed, among other things.

5.1 Comparable requirements in ICT project management

The basic requirements for an ICT project methodology (Art. 15 RTS RMF), which are to be implemented on the basis of a corresponding guideline, are also contained in the RTS RMF (Art. 15 para. 1 - 3 RTS RMF), analogous to para. 7.3 BAIT/ para. 7.4 VAIT. There are simplifications when considering correlations across several projects. To date, BAIT/VAIT have stipulated that a risk assessment regarding the dependencies of IT projects with each other. DORA no longer requires this consideration. Instead, projects must be assessed taking into account the impact on critical and important functions and communicated to the management body depending on the importance and size of the project (Art. 15 para. 5 RTS RMF).

Further simplifications result from the elimination of the requirements for qualitative and quantitative resources as well as restrictions in the information security view, which only requires compliance with the protection objectives (Art. 15 para. 1 RTS RMF). Requirements relating to project documentation and lessons learnt are also not part of the RTS RMF.

5.2 Detailed specifications for ICT system procurement, development and maintenance

Compared to the BAIT/VAIT, the RTS RMF is much more detailed and contains specific minimum components for a guideline on procurement, development and maintenance (Art. 16 para. 1 RTS RMF). In contrast to BAIT/VAIT, the focus is less on the documentation of the application development and instead more on the secure implementation (Art. 16 para. 1 lit. a and c RTS RMF) and the identification of the requirements needed to implement the application (Art. 16 para. 1 lit. b RTS RMF). Complete documentation of requirements in the sense of a technical concept or specifications is not explicitly required.

The RTS RMF describes in great detail the measures to be taken t o test IT systems (Art. 16 para. 2 RTS RMF). In future, for example, security tests will be required as part of the source code review for systems and applications with internet connectivity (Art. 16 Para. 3 RTS RMF).

In contrast, the VAIT only require the introduction of a control process at this point, without naming specific test procedures or scenarios.

Compared to the BAIT/VAIT, there are no longer any requirements for stress scenarios or documentation of the tests. However, Art. 17 RTS RMF requires an effective test procedure

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

(Chapter 13 MaGo) are also considered due to the close interrelationship with the requirements of BAIT and VAIT.

Chapter V of DORA regulates the use of ICT services provided by third-party ICT service providers. A number of key principles for the sound management of ICT third-party risk are defined for this purpose. These include requirements for governance, the life cycle of an ICT service procurement, the handling of certain ICT third party risks and the minimum contract content. A list of the minimum contract contents can be found in the annex to these implementation guidelines.

6.1 Differentiation from outsourcing and outsourcing

ICT third party risk management in accordance with DORA supplements the existing sectoral regulations on outsourcing or outsourcing[6] (hereinafter referred to as "outsourcing"). The sector-specific outsourcing requirements must therefore continue to be observed, i.e . both the statutory requirements and the requirements from MaRisk or MaGo, for example, continue to apply; they exist in parallel and complement each other. As a result, it must be assumed that in many cases a contractual agreement on the use of
ICT services also constitutes outsourcing (and vice versa). The supervisory authorities are striving to harmonise the requirements for ICT third party risk management under DORA and the sectoral requirements for outsourcing.

For this reason, this chapter of the implementation notes not only considers the main effects of the differences between DORA and BAIT/VAIT, but also the relevant sections of MaRisk and MaGo.

The definition of contractual agreements for the use of ICT services (Art. 28 para. 1 lit. a in conjunction with Art. 3 no. 21 DORA) is significantly broader than the previous outsourcing definitions, in particular because it applies to all types of outsourcing for financial companies. "ICT services for the performance of their business activities". This makes it necessary to assess all ICT-related third-party purchases and may result in uncertainties regarding the correct classification during implementation. In addition, in many cases an expansion of the circumstances to be covered is to be expected.

Of particular importance for the scope of the requirements to be fulfilled is whether the purchased ICT service supports a critical or important function. In such a case, it is assumed that the associated ICT third-party risks are of particular importance. The assessment of functions as "critical or important" is not identical in terms of methodology and content to a materiality assessment for outsourcing[7] . It is based on the impact that a failure or limited performance of the function would have (Art. 3 No. 22 DORA). Here too, the development of suitable criteria for categorisation (Art. 3 para. 2 RTS TPPol) and the assessment of all circumstances is necessary.

Machine translation courtesy of PRIVACY CRAFT

management of third party ICT risk [...]. These principles complement the sector-specific legislation applicable to outsourcing."

[7] Or assessment of whether an important function or insurance activity within the meaning of the VAG exists.

6.2 Extension of contract requirements

DORA is accompanied by a significant expansion of the contractual content that must be agreed with the ICT third-party service provider[8] . These are in particular

- Formal requirements, including form and illustration in a document (Art. 30 para. 1 DORA and Art. 8 para. 4 RTS TPPol),
- Minimum content for all contractual agreements (Art. 30 para. 2 DORA),
- Minimum content for contractual agreements to support critical or important functions (Art. 30 para. 3 DORA and Art. 8 ff. RTS TPPol),
- Cancellation rights (Art. 28 para. 7 DORA and Art. 7 RTS-E SUB),
- relevant contractual content for requirements from Art. 1 para. 1 lit. a and other relevant laws (Art. 8 para. 1 RTS TPPol),
- Examination and, if applicable, testing rights (Art. 8 para. 1 RTS TPPol in conjunction with Art. 1 para. 1 lit. a point iv DORA, Art. 8 para. 2, Art. 8 para. 3 lit. g and h as well as Art. 3 para. 8 lit. c and d RTS TPPol),
- Obligation to replicate the relevant contract content in subcontracting to support critical or important functions (Art. 3 para. 1 lit. c RTS-E SUB),
- Description and conditions under which subcontracting is permitted (Art. 30 para. 2 lit. a DORA, Art. 4 RTS-E SUB),
- a sufficient notification period in the event of significant changes to subcontracts for critical or important functions and an obligation not to implement any changes within this period, as well as the right to request changes (Art. 6 para. 1, 3 and 4 RTS-E SUB) and
- Measures and key indicators for monitoring performance, information security requirements and compliance with guidelines and processes of the financial organisation and, where appropriate, contractual penalties (Art. 9 para. 1 RTS TPPol).

Due to the significant expansion of the scope of application and the mandatory contractual content, in many cases it will be necessary to renegotiate or renegotiate a large number of contracts with third-party ICT service providers. In addition, the mandatory contract contents also cover contractual agreements that do not support critical or important functions or do not relate to significant outsourcing .[9]

Standard contractual clauses developed by authorities for certain services should be taken into account when concluding contracts (Art. 30 para. 4 DORA). However, no standard contractual clauses are currently available, so supervised companies should not wait for the publication of standard contractual clauses to implement the minimum contract content.

[8] The list only includes requirements that are explicitly presented as minimum contractual content at Level 1 or Level 2. Other contract contents that result from other requirements or that should be agreed upon were not included.

[9] or assessment of whether an important function or insurance activity within the meaning of the VAG exists.

There are no extended transition periods for the adaptation of existing contractual agreements (risk analyses, contractual content). Art. 3 para. 1 RTS TPPol indicates that there should be a documented implementation schedule and that implementation should take place in good time. The contractual agreements should be adapted as soon as possible.

6.3 New regulation of subcontracting

Subcontracting for critical or important functions is comprehensively regulated in the RTS-E SUB, which was published in draft form at the beginning of December[10] . The RTS significantly expands the breadth and depth of regulation:

- The financial undertaking must assess whether the third-party ICT service provider is able to select a subcontractor appropriately and monitor it appropriately (Art. 3 para. 1 RTS-E SUB).
- Contract contents relating to subcontractors (Art. 4 RTS-E SUB).
- Documentation and monitoring of subcontracting chains (Art. 5 RTS-E SUB).
- Procedure in the event of material changes (Art. 6 RTS-E SUB) and any associated cancellation rights (Art. 7 RTS-E SUB).

6.4 Extensive requirements for risk analyses and due diligence

The scope of the requirements for risk analyses and due diligence, particularly for contractual agreements that affect critical or important functions, has increased. This primarily concerns the content and depth of the analysis. The content for
ICT services that do not support critical or important functions are only provided in a very generalised manner:

- Assessment of compliance with regulatory conditions (Art. 28 (4) DORA),
- Identification and assessment of all relevant risks, including ICT concentration risk (Art. 28 (4) DORA),
- Suitability of the ICT third-party service provider as part of due diligence (Art. 28 para. 4 DORA),
- Identification and assessment of conflicts of interest[11] (Art. 28 para. 4 DORA) and the
- Compliance with appropriate information security standards (Art. 28 para. 5 DORA).

In the case of ICT services that support critical or important functions, there are additional issues to be analysed that exceed the previous requirements in terms of scope.
z. significantly in some cases:

[10] As the RTS for subcontracting is in the group of RTS/ITS with a processing time of 18 months, changes can still be expected after the consultation deadline on 4 March 2024.
[11] For ICT services that support critical or important functions, also Art. 7 RTS TPPol.

- Specification of a minimum catalogue of risks to be considered as part of the ex-ante risk analysis, including operational risks, legal risks, ICT risks, reputational risks, confidentiality and data protection risks, risks relating to the availability of data, risks relating to the location of data processing and storage, location of the third-party ICT service provider, concentration risk (Art. 5 para. 2 RTS TPPol).
- Specification of a minimum catalogue of factors that the ICT third-party service provider should fulfil, including reputation, capabilities, ICT risk management, subcontracting, location, auditability, ESG requirements (Art. 6 para. 1 RTS TPPol).
- Weighing up the benefits and risks associated with subcontracting (Art. 29 para. 2 DORA, Art. 1 RTS-E SUB) and evaluation of long and complex chains of subcontracting (Art. 29 para. 2 DORA).
- Consideration of legal risks, i.e. the provisions of insolvency law (Art. 29 para. 2 DORA) and, in the case of third countries, compliance with and enforceability of legal provisions and compliance with data protection regulations (Art. 29 para. 2 DORA).
- Assessment of whether the ICT third-party service provider has sufficient resources to comply with legal and regulatory requirements (Art. 3 para. 4 RTS TPPol)
- Appropriate consideration of "the latest and highest quality standards for information security" (Art. 28 para. 5 DORA).

Likewise, in the case of critical or important functions, test or assessment results of the ICT third-party service provider must also be used as part of the due diligence, insofar as appropriate, before the contract is concluded (Art. 6 para. 3 lit. a and b RTS TPPol). The provision of such audit or assessment reports is likely to pose challenges for some third-party service providers.

6.5 Changed requirements for the exit

The requirements for exit strategies/plans for ICT services to support critical or important functions are increasing significantly, in particular the expectations regarding the objectives of the exit strategies have been significantly expanded (Art. 28 para. 8 DORA). Financial companies should be able to withdraw from contractual agreements without interrupting their business activities and without affecting the services they provide to customers or their compliance with regulatory requirements. The exit plans should be based on plausible scenarios and reasonable assumptions (Art. 10 RTS TPPol). In addition, the exit plans must be sufficiently tested and should be reviewed regularly.

The previous opening clause for intra-group or intra-network outsourcing at credit institutions (waiver of exit processes in accordance with AT 9 para. 15 d MaRisk) no longer applies if these are also ICT services. However, proportionality can still be taken into account in relation to a reduced risk (insofar as applicable) (Art. 1 lit. e RTS

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."

Explanations of BAIT/VAIT as minimum requirements for appropriate information security measures and processes.

Art. 11 RTS RMF requires data and system security measures to ensure that:

- hardening measures are taken and these are checked regularly,
- software and mobile data carriers are only used after permission has been granted (white list approach),
- Regulations for mobile working exist with regard to authorised devices and software,
- procedures are in place for the secure deletion of information and destruction of data carriers, and
- measures are implemented to protect against the intentional or accidental loss of data.

In addition, stricter requirements apply to ICT systems that are operated by third-party ICT service providers. This includes

- that manufacturer recommendations are implemented on ICT systems operated by the Institute,
- information security roles and responsibilities are clearly defined between the financial organisation and the third-party ICT service provider,
- sufficient skills remain in the financial organisation to manage and secure the ICT solution used, and
- technical and organisational measures have been implemented to reduce the risks posed by the use of the third-party ICT service provider on the company's own infrastructure.

7.1 Strengthened network security

Art. 13 RTS RMF contains requirements regarding network security that are already known from chapters 4.3 and 5.2 BAIT/VAIT. These include detailed requirements on, for example, network segmentation and segregation, network access control and third-party device detection, hardening of all network components and reviews of the network architecture. A greater implementation effort is assumed in the realisation of the requirement in Art. 9 para. 4 lit. b DORA for the automated isolation of information assets in the event of cyber attacks. These are further specified in Art. 13 para. 1 lit. j RTS RMF.

With increasing demands on network security, the role of firewalls is also being emphasised more strongly. Accordingly, a life cycle with defined roles and responsibilities as well as firewall recertification must be defined for firewall rules (Art. 13 para. 1 lit. h RTS RMF). Firewall rules that support critical or important functions in ICT systems must be recertified at least every six months, analogous to the regulations in access management.

The protection of information during transmission (in transit) is particularly emphasised in Art. 14 RTS RMF. However, no specific requirements are made here, but guidelines and procedures are required to ensure this, taking into account the risk profile (Art. 14 para. 2 RTS RMF). According to Art. 14 para. 1 lit. c RTS RMF, it is also new that for risks that cannot be technically mitigated, confidentiality declarations or confidentiality agreements are required. Non-disclosure agreements (NDAs) must be concluded with employees of the financial company as well as with the affected employees of the ICT third-party service providers.

7.2 Encryption of data even during processing

Art. 9 DORA and Art. 6 and 7 RTS RMF place significantly higher requirements on the encryption of information compared to para. 5.2 BAIT/VAIT. It is required that data must be encrypted in all states (at rest, in transit & in use) according to its criticality. While the requirements f o r encryption of stored data and during transmission in accordance with protection requirements are stipulated in para. 5.2 BAIT/VAIT, the requirement under Art. 9 para. 2 DORA for encryption of data during processing "in use" is a novelty that is likely to involve considerable implementation effort. For these requirements, in cases where encryption during processing is not possible, data must be processed in separate and specially protected environments or other suitable measures must be taken.

What is also new is that cryptographic keys, which were previously not directly addressed in BAIT/VAIT, are now dealt with specifically in Art. 7 RTS RMF. A policy and procedure for handling cryptographic keys and measures to protect them must be established. The entire life cycle from generation to destruction must be taken into account. If keys are lost, damaged or compromised, it must be ensured that they can be replaced. In accordance with Art. 7 para. 4 RTS RMF, an up-to-date register of all certificates and certificate stores must be kept at least for those ICT assets t h a t support critical or important functions.

7.3 Prompt detection and treatment of vulnerabilities

The prompt identification, handling and treatment of vulnerabilities is regulated in Art. 10 RMF RTS. Accordingly, financial companies must ensure that

- ICT third-party service providers address vulnerabilities affecting the ICT systems of financial organisations and report them to the financial organisation in a timely manner in the event of critical vulnerabilities and statistics and trends,
- weaknesses are also communicated responsibly and appropriately to external parties and, if necessary, the public,
- automated vulnerability scans are performed for timely identification, with at least a weekly vulnerability scan required for ICT systems that support critical and important functions,

- third-party and open-source software libraries should also be included in the vulnerability process.

Vulnerabilities must be remedied in accordance with a prioritisation developed by the financial company (Art. 10 para. 2 lit. f RTS RMF), taking into account the criticality of the vulnerability, classification of the asset and the risk profile. The patching of vulnerabilities must be prioritised over other measures. Where possible, available software and hardware patches and updates must be identified and assessed using automated tools (Art. 10 para. 4 lit. a RTS RMF). A separate procedure must be drawn up for the installation of patches in "emergencies" (Art. 10 para. 4 lit. b RTS RMF). If patches are not installed within the specified deadlines, a defined escalation procedure must be initiated (Art. 10 para. 4 lit. d RTS RMF).

The threats to the information network known from Art. 5.3 BAIT/VAIT are not identified in DORA via "potentially security-relevant information", but via "anomalous activities" (Art. 10 DORA).

Supported by suitable procedures, anomalous activities and behaviour must be detected (Art. 10 para. 1 DORA), early warning indicators (Art. 17 para. 3 lit. a DORA) identified and all detection mechanisms regularly tested (Art. 25 DORA), which must be processed within a predefined period during and outside regular working hours (Art. 23 para. 2 lit. c RTS RMF). Sufficient technical and organisational resources should be planned for this.

For the sake of completeness, it should be mentioned that within ICT risk management, DORA refers to extensive additional requirements for the handling, classification and reporting of ICT-related incidents (cf. Chapter III, Art. 17 - 23 DORA) and testing (cf. Chapter IV, Art. 24 - 27 DORA). However, Chapters III and IV DORA are not the subject of these implementation instructions. However, it has been recognised that the detection of anomalous behaviour in particular goes beyond the previous strongly use case-driven approach of Chapter 5.4 BAIT/VAIT.

Extensive logging requirements are set out in Art. 12 RTS RMF as the basis for recognising anomalous activities.

- The retention period for logs depends on the business and security requirements, the purpose of retention and the risk profile of the ICT assets concerned. It is important that the decision is sufficiently justified and documented.
- Logs must be protected against manipulation and deletion. The failure of the log function must be monitored and failures must be recognised.
- All of the financial company's ICT systems must be synchronised with a reliable reference time.

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