DORA - Delta View

What is really new from DORA for the established financial industry

Dr Waldemar Grudzien
Katrin Miller
Theresa Sporn
Moritz Treutwein

October 2022
Blogpost

Key Facts

- Previous BaFin supervisory objects are well equipped for DORA, new DORA supervisory objects face major tasks
- New for BaFin supervision objects are 24 requirements from the directive text and for all DORA supervision objects 19 RTS[1] as well as 2 ITS[2]
- Many RTS/ITS can be brought forward, waiting for final versions is not recommended
- Requirements can be bundled over time with RTS/ITS and resolved early
- DORA underpins pro-cloud decision in regulatory terms, as a "-supervisory shadow" is finally history with DORA

1. Introduction

In the future, DORA is to transfer national regulations in the area of financial market regulation into uniform, harmonised EU law. CORE has already outlined the nature, content, effects and recommendations in a first blog post on DORA. This blog post is a supplement to the first and focuses on the delta to the current regulation, i.e. what is actually new for the established financial industry from DORA.

DORA expands the scope to about 20 types of companies and ICT third party providers[3]. For those companies for which the rule contents such as ICT risk management, reporting of ICT incidents and auditing of digital operational stability were previously not an issue, everything is new from DORA. For the companies already supervised by BaFin, such as credit institutions, financial services institutions, payment institutions and e-money institutions, insurance companies,

[1] Regulatory Technical Standards
[2] Implementing Technical Standards
[3] Approx. 20 types, since in the current trilogue version of 23.06.2022, compared to the previous version of 26.09., "Statutory auditors and audit firms" (letter q) have been removed.2020, "statutory auditors and audit firms" (letter q) have been removed: (a) credit institutions, (b) payment institutions, (c) electronic money institutions, (d) investment firms, (e) crypto service providers, issuers of crypto securities, issuers of asset linked tokens and issuers, significant asset linked tokens, (f) central securities depositories, (g) central counterparties, (h) trading venues, (i) trade repositories, (j) alternative investment fund managers, (k) management companies, (l) data provision services, (m) insurance and reinsurance undertakings, (n) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, (o) institutions for occupational retirement provision, (p) credit rating agencies, (~~q) auditors and audit firms, (~~r) critical benchmark administrators, (s) crowdfunding service providers, (t) securitisation registries, (u) third party ICT providers.

securities institutions and capital management companies, DORA contains many parts that they already have to fulfil from other regulatory standards (see Figure 1).

Financial entitiesand ICT third-party providers: Legal basis for special audits of technical and organisational equipment

Companies	Legal basis for special audit	Legal basis for techn.-organ. equipment	BaFin XAIT	BaFin Minimum requirements(MaX)
I Credit institutions, financial services institutions	§ Section 44 (1) KWG	§ Section 25a (1) KWG	BAIT from 16.08.2021	MaRisk from 16.08.2021
I Payment institutions and e money institutions	§ Section 19 (1) ZAG	§ Section 27 (1) CISA	ZAIT from 16.08.2021	No own MaX document
II Insurance companies	§ 306 para. 1 VAG	§ 294 par. 4 VAG	VAIT from 03.03.2022	MaGo from 02.03.2018
III Securities institute	§ Section 41 WpIG	-	BAIT from 16.08.2021	MaRisk from 16.08.2021
IV Capital management companies	§ 14 KAGB (by reference to § 44 KWG)	§§ Sections 28, 29 and 30 of the German Investment Code (KAGB)	KAIT from 01.10.2019	KAMaRisk from 10.01.2017
V Third-party ICT providers	Articles 33, 34, 35 DORA (draft of 23.06.2022)	Article 1 DORA (draft of 23.06.2022)	-	-

Figure 1: Special audit in financial companies - legal basis and new object of supervision ICT third party providers

Other regulatory standards known to the aforementioned group are the IT Security Act 2.0 with the two central requirements "minimum security of technical-organisational equipment" and "reporting system for serious security incidents" (only for systems considered KRITIS), the Financial Market Integrity Strengthening Act (FISG) with provisions on the notification requirement for material outsourcing, the PSD 2 for payment service providers with the RTS for increased security requirements in online payment transactions and the Business Secrets Act (GeschGehG) in the event of claims for damages from successful attacks. The entirely new parts will be discussed in the follow-up.

The new requirements are fed from two sources: the text of the regulation and the RTS and ITS. The RTS and ITS are also components of the regulation, but due to their later completion they form a class of their own. DORA is expected to enter into force at the turn of 2022/23, with the RTS/ITS following 12 to 18 months later. The application of DORA follows two years after its entry into force, so that the supervisory objects will have 6 to 12 months to implement the published RTS/ITS.

2. Need for action from the text of the directive

In Figure 2 all requirements from DORA are compiled that are new for the supervisory objects from XAIT[4] and MaX[5] already supervised by BaFin - in short: "DORA-Delta". A detailed tabular list of the DORA delta can be found in the appendix.

A to B: Overarching Requirements | **C to M**: Requirements for ICT risk management | **N to O**: Reporting of ICT incidents | **P to S**: Testing of digital operational stability | **T to X**: Testing for risk from ICT third party

Delta	Topic	Source
A	8(2): CIA protection of data and systems	Author recommendation
B	Establishment of a certifiable ISMS	Author recommendation
C	Creation of a separate "Digital Resilience Strategy"	Article 5 (9)
D	Checking the option to delegate the verification of compliance with ICT risk management requirements to third parties	Article 5 (10)
E	Regular, but at least annual, ICT risk assessment from ICT legacy systems	Article 7 (7)
F	Creation of an "Information Security Policy"	Article 8 (4)
G	Detection of anomalous activity, including ICT network performance problems and ICT incidents & Detection of trading information anomalies	Article 9 (1), Article 9 (4)
H	Creation of an "ICT strategy for the continuation of business operations"	Article 10 (1)
I	Definition of crisis management function	Article 10 (6)
J	Reporting of costs and losses from ICT incidents to the competent authority (BaFin)	Article 10 (9)
K	Specific obligations for central counterparties and central securities depositories for recovery plans and the secondary processing location	Article 11 (3,4,5)
L	Reporting of changes from ICT incidents to the competent authorities	Article 12 (2)
M	Assign at least one person to implement the communication strategy and act as an external spokesperson.	Article 13 (3)
N	All financial entities must report serious ICT incidents	Article 17 (1,3)
O	If a serious ICT incident has or could have an impact on service users and customers, financial entities must inform them immediately	Article 17 (2)
P	Establish a programme to annually audit the digital operational stability of all critical ICT systems and applications.	Article 21 (6)
Q	Threat-oriented penetration tests	Article 23
R	Checking the suitability of the testers	Article 24 (1)
S	Use of internal testers is subject to three conditions	Article 24 (1a)
T	Creation of a "Strategy for Risks from ICT Third-Party Providers"	Article 25 (3)
U	Informing the competent authority of theplanned procurement of contracts for critical or important functions	Article 25 (4)
V	Preparation of exit plans and their "sufficient" testing	Article 25 (9)
W	Assessment of ICT concentration risk	Article 26
X	Essential contents of the contract	Article 27

Figure 2: Delta from DORA draft of 23.06.2022

[4] XAIT combines BAIT, KAIT, VAIT and ZAIT into one generic term

[5] MaX summarises minimum requirements for risk management: MaRisk, MaGo and KaMaRisk

3. Need for action from RTS / ITS

Figure 3 summarises all RTS and ITS resulting from DORA. All RTS and ITS will be finalised by ESA 12 to 18 months after DORA enters into force, so in theory the oversight objects cannot start implementation until these final versions are available. But bringing forward various RTS and ITS is possible and necessary in order to be better prepared for the DORA than the business community was, for example, with the GDPR. Furthermore, spreading all RTS and ITS over the available two years leads to a more comfortable processing situation than if work is only started when these 21 requirements are ready. In this case, the companies would only have 6 months for the implementation of 8 RTS/ITS.

RTS ITS

	Article	Topic RTS / ITS	When after entry into force
1	14(a)	8(2): CIA protection of data and systems	1 year
2	14(d)	8(4) lit. c: Identity and access management, incl. physical access protection, monitoring of abnormal behaviour	1 year
3	14(e)	9(1) (2): ICT-related incident detection, SIEM, SOC	1 year
4	14(f)	10(1): ICT business continuity plan as part of the operational business continuity strategy	1 year
5	14(g)	10(5): Annual review of the ICT disaster recovery and business continuity plan.	1 year
6	14(h)	10(3): Components of the ICT disaster recovery plan to be independently audited	1 year
7	14(ha)	5(6) Content and form of the report on the review of the ICT risk management framework	1 year
8	14a(3) lit. a until e	All contents from 14a(1 lit. a,c,f,g), contents and the format of the report on the review of the ICT risk management framework according to 14a(2)	1 year
9	16(3)	16(2) lit. a: Criteria for determining serious ICT incidents with mandatory reporting, proportionality principle under Article 31(2)	1 year
10	16(3)	16(2) lit. b: Criteria on the relevance of serious ICT incidents in other countries	1 year
11	16(3)	16(2) lit. c: Take into account user and transaction numbers for materiality thresholds of significant cyber threats, among others	1 year

	Article	Topic RTS / ITS	When after entry into force
12	18(1) lit. a	Content of reports on serious ICT incidents, deadlines and content for reports	18 months
13	18(1) lit. b	Standard forms, templates and procedures for reporting a serious ICT incident	18 months
14	23(4)	Details on penetration testing according to TIBER-EU	18 months
15	25(10)	Standard template for information registers on contracts with ICT third-party providers	1 year
16	25(11)	Policy on the use of ICT services incl. multi-vendor strategy	1 year
17	27(4)	(2) lit. a Description of all functions and services to be provided by the ICT third party provider, incl. admissibility for subcontracting.	18 months
18	36(1) lit. a	Information for voluntary application of the ICT third party provider	18 months
19	36(1) lit. b	off 31(1): Content and format for final reports on the implementation of measures	18 months
20	36(1) lit. ca	from 31(1): Information, incl. structure, formats and methods, that a third-party ICT provider must submit; criteria for composition of the audit team incl. designation, tasks and working modalities	18 months
21	36(1) lit. d	from 37(2): Assessment of the actions of the ICT third party providers on recommendations of the lead supervisor	18 months

Figure 3: Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) resulting from DORA

Those technical standards that supervisory objects must already have in the field today should at least be updated, or if not adequately available, brought up to a legally compliant level. This includes all seven RTS from Article 14, because the existing BaFin supervisory objects from XAIT and MaX have to deal with the protection of confidentiality, integrity and availability (CIA) anyway, and all new supervisory objects from DORA have to do so for their own sake. For all new components from these RTS, such as the content and form of the report on the review of the ICT risk management framework, lobbying in the form of making one's own industry, sector, country-wide or even European coordinated drafts available to the ESA is a good idea, so that the "surprise" when the RTS is presented by the ESA remains as small as possible.

The same applies to the three RTSs from Article 16 around serious ICT incident reports and the one RTS and the one ITS from Article 18 on serious ICT incident reports: firstly, they all have to act on incidents and secondly, the criteria to be elaborated should be sent to the ESA beforehand as an agreed discussion proposal. In this double sense - own implementation and lobbying for a preferably Europe-wide, but at least nationally harmonised discussion proposal to the ESA - all other RTS and ITS from Figure 3 can also be seen in this light.

Supervised entities can already prepare for the RTS from Article 23(4) on penetration testing, as the regulation favours the TIBER-EU testing regime, which is known and understood. Only the requirements for internal testers could bring surprises from the RTS, so that apart from securing external test capacities, internal test resources continue to do their day's work until the RTS.

Registers with contracts with outsourcing companies are also known, so that only an adaptation to the specified format is required here for the RTS from Article 25(10). The policy on the use of ICT services required by Article 25(11) should already be a component of an ISMS and should not pose any major hurdles for existing supervisory objects. This should also apply to the detailed description of all functions (Article 27(4)) of the outsourcing company, otherwise things would already be going wrong in the contracts between the BaFin supervisory object and the hyperscaler. With the voluntary application of the ICT third party provider to be included in the list of ICT third party providers to be supervised (Article 36(1)(a)), the third party provider can only apply after the corresponding RTS has been published. This also applies to the last three topics 19 to 21 from Figure 3: Adaptation to the legal text only makes sense once the RTS has been published.

4. Recommendations for action for previous supervisory objects

In Figure 4, the RTS/ITS "1" to "21" from Figure 3 are thematically assigned to the requirements from DORA regulation text "A" to "X" from Figure 2 and plotted together over the time axis. The assumed date of entry into force of DORA is 1 January 2023.

The 21 RTS/ITS are accompanied by Figure 4 two further "deadline matters" 22 and 23 from the text of the directive. Although these are not RTS/ITS, they contribute to their further concretisation:

- 22: Article 10(9a): Common guidelines of the ESAs for estimating the aggregated annual costs and losses referred to in paragraph 9.

- 23: Report from Article 19 (1) in conjunction with (3). Para. 3: Report on the examination of an EU platform for serious ICT incidents

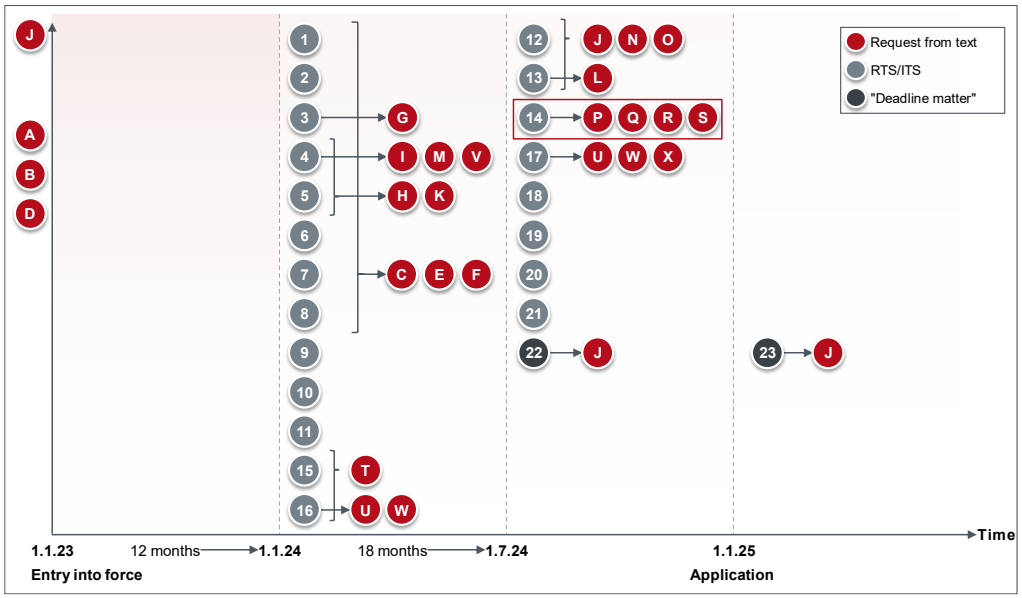

Figure 4: Merger of directive articles and RTS/ITS over time axis

From Figure 4 the possibility of combining the requirements from the directive text and RTS/ITS becomes crystalline across the time axis, so that the work on conformity with DORA can be bundled and thus better distributed in terms of time and organisation. A consideration at group level opens up spaces of focus.

Group A, B, D:

- A: Timely engagement with the philosophy, systematics and anticipation of DORA for one's own organisation is critical for success
- B: Previous BaFin supervisory objects must have a fully comprehensive ISMS in operation anyway - check for up-to-dateness recommended
- D: Checking the option to outsource 2nd line can be done in advance

Group C, E, F:

- C: The digital resilience strategy includes all requirements of Article 14 DORA and thus 8 RTS - to be done in the context of the ISMS update
- E: Based on own definition Identification of legacy ICT systems and joint treatment in strategy from C)
- F: Information security policy to be derived from existing IT strategy and new strategy from C)

Group I, M, V:

- I: Defining the crisis management function in the operational business continuity strategy
- M: Determine function Implementer of the communication strategy in the operational strategy to continue business operations

- V: Exit plans and their testing embedded in the operational strategy to continue business operations

Group H, K:

- H: Preparation of ICT strategy for the continuation of business operations and its review along the guard rails from RTS 4 and RTS 5
- K: Specific obligations for secondary processing location for CSDs and central counterparties along the guard rails from RTS 4 and RTS 5

Group U, W and X:

- U: Reporting of outsourcing/projects known from FISG, but RTS 16 and RTS 17 will impose new requirements
- W: ICT concentration risk assessment esp. difficult to prepare earlier without RTS 16
- X: RTS 17 will set new requirements for essential contract content

Group J, N, O:

- J: immediate lobbying against deadline matter 23 recommended; with RTS 12 and RTS 13 as well as deadline matter 22, the content and format of this notification will be prescribed
- N: immediate lobbying necessary; with RTS 12 and RTS 13, the content and format of this notification will be prescribed
- O: immediate lobbying necessary; with RTS 12 and RTS 13, the content and format of this notification will be prescribed

Group P, Q, R, S:

- P: Elaboration of the testing programme must start immediately, RTS 14 will detail penetration tests
- Q: Elaboration of procedure for sufficient equipment with external and, if planned, also internal test capacities; elaboration of testing on live systems, early securing of test capacities recommended
- R: Selection and securing of the testers with the inclusion of RTS 14 - but orientation to TIBER EU already now possible and recommended
- S: Decide whether internal testers still make sense in the light of the requirements.

Single deltas:

- G: Connect anomaly detection with RTS 3
- L: Reporting of lessons learned does not require premature action
- T: Link strategy for risks from ICT third-party providers with specifications on multi-vendor strategy from RTS 16; RTS 15 will structure the contract register

Conclusion

DORA will broaden the supervisory framework to about 20 types of companies, finally putting Europe's focus on the most important resource for prosperity and creative freedom in an over-complex world - the digital infrastructure. Financial companies and ICT third parties are the starting point for a modern, automated supervisory practice. Other important sectors will follow.

All in all, both the existing BaFin supervisory objects and the new DORA supervisory objects cannot afford to wait for the completion of the RTS and ITS by the ESA towards the end of 2023 and towards the middle of 2024. As explained above, in this case the companies have a maximum of one year, for 8 RTS/ITS even only 6 months, for implementation. Secondly, this necessary supervisory work unduly blocks line activities for many months; stretching the time from 6 months to up to two years is more promising than waiting. Rather, both groups must start preparing for them now. Then, firstly, they have the chance to remain legally compliant and, secondly, on the basis of their lessons learned from DORA, they can submit discussion offers for individual RTS and ITS to the ESAs in good time in order to still be able to influence the design of details in governance and organisation of their digital production base.

Away from regulatory policies and the supervisory "small stuff", new insights and questions arise with DORA. First of all, the commonplace: banking supervision is IT supervision! This realisation should now have arrived everywhere. With DORA at the latest, the "supervisory shadow" that the supervisory objects had in the first years of out-sourcing to the cloud disappears. Conversely, however, this means that outsourcing to the cloud is well thought out and calculated, because going to the cloud only makes sense if there is real added value, as the "advantage" of lower compliance requirements in the cloud no longer exists with DORA. If a company now outsources according to the conditions of DORA, then the probability of success of the outsourcing is greater because of DORA than without DORA. A reverse conclusion in the direction of supervision: If the same supervisor supervises financial companies and ICT third-party providers according to the same rules, why do financial companies have to control and supervise these ICT third-party providers as if they were not supervised?

5. Annex: Chenges from DORA for BaFin supervisory objects

No.	New field of action	Description / Conclusion	Source
Overarching requirements			
A	Preparation of time and action plan for all RTS still to be prepared	Early preparation for the topics of the RTS and ITS (see chapter 3) before their completion is strongly recommended.	Recommendation of the authors
B	Establishment of a certifiable ISMS	ISMS no longer required in DORA version of 23.06.2022, however DORA requires a fully comprehensive ISMS in practice. So far, the XAIT requirements call for the operation of an ISMS in each case in the preliminary remark, but not a certified ISMS. In order for the ISMS to meet all regulatory requirements, it must be certifiable, i.e. "as if" certification, for example according to ISO 27001, were the goal. Secondly, the authors assume that in a further round of regulation, a certified ISMS will be prescribed for the critical processes.	Recommendation of the authors
ICT risk management requirements (Articles 5 to 14)			
C	Creation of a separate "Digital Resilience Strategy	Emphasis on digital resilience. This newly required strategy is part of the ICT risk management framework and combines already known content from documents such as the IT strategy, information security guideline and outsourcing guideline. However, this strategy must be written as a stand-alone document, continue the business strategy into ICT and focus specifically on ICT risks.	Article 5 (9)
D	Consider the option of delegating the verification of compliance with ICT risk management requirements to third parties.	Financial companies can delegate the aforementioned review externally and thus, for example, relieve the internal audit department.	Article 5 (10)
E	Regular assessment of ICT risk through ICT legacy systems	The finance company must clarify which parts of the infrastructure are considered legacy ICT systems. The reference from DORA "before and after connection of old and new technologies, applications or systems" shifts the demarcation "old/new" to further components of an infrastructure.	Article 7 (7)
F	Creation of an "Information Security Policy	This policy is intended to set out the rules for protecting the CIA's protection objectives and is therefore to be understood as a guideline rather than a strategy. In practice, every regulated financial company has these rules in the form of the Target Measures Catalogue (TMC) and the associated controls, as well as in guidelines and work instructions for the protection of assets, but this document is explicitly mentioned, so it must be created as an overarching 'bracket policy',	Article 8 (4)

No.	New field of action	Description / Conclusion	Source
		as a separate strategy or, if applicable, as part of the IT strategy.	
G	Detection of anomalous activity, including ICT network performance problems and ICT incidents	New if supervision always means a SIEM and/or SOC	Article 9 (1)
	Detection of anomalies in trade reports	New, only for investment firms. According to MiFIR, these must use so-called Approved Publication Arrangements (APA) and can use so-called Approved Reporting Mechanisms (ARM).	Article 9 (4)
H	Creation of an "ICT strategy for the continuation of business operations	The components of this "strategy" must also already be present in the BCMS (Business Continuity Management System) today, but the supervisory authority considers the ICT components to be so critical to operations that they are now being highlighted. From the authors' point of view, this ICT strategy can be part of the BCM strategy and address IT content exclusively.	Article 10 (1)
I	Definition of crisis management function	This function is the typical BCM management function, but is now required by law.	Article 10 (6)
J	Reporting of costs and losses from ICT incidents to the competent authority	Politically prevented for decades (keyword UP KRITIS). Financial companies must clarify internally according to which metrics they can compile ICT incidents, costs and losses. Externally, the question of the dangers from this central collection remains. Here, lobbying via associations and other industry groups will be necessary as political flanking.	Article 10 (9)
K	Specific obligations for Central Counterparties and Central Securities Depositories for recovery plans and secondary processing location	Detail specifications for backups, restart and second processing location for two of the 20 types of financial companies.	Article 11 (3,4,5)
L	Reporting changes from ICT incidents to the competent authorities	This reporting of lessons learned from ICT incidents to the competent authorities is new and puts them in a better position to have their finger on the pulse of attacks and threats to their supervisory objects.	Article 12 (2)
M	Assign at least one person to implement the communication strategy and act as an external spokesperson.	The codification of a responsible role as "public spokesperson and media spokesperson" is new. Large companies have spokespersons even today. Many companies newly supervised from DORA will have to designate this role in the first place.	Article 13 (3)
N	All financial companies must report serious ICT incidents.	Up to now, only CRITIS operators have to report serious ICT incidents to the competent authority in accordance with the IT Security Act in conjunction with BAIT Chapter 12 or VAIT Chapter 11 or ZAIT Chapter 12. With DORA, this reporting	Article 17 (1, 3)

No.	New field of action	Description / Conclusion	Source
		group is extended to all financial companies according to Article 2 para. 2.	
O	ICT incident notification: If a serious ICT incident has or could have an impact on service users and customers, financial entities must notify them immediately.	Service users and customers must be informed of serious ICT incidents. This duty to inform has so far only been known from the GDPR, but with DORA it is now also extended to information and cyber security.	Article 17 (2)
P	Establish a programme to annually audit the digital operational stability of all critical ICT systems and applications.	Two very important aspects are new: firstly - with one exception - the annual cycle of the audit and secondly, the audit must cover all critical systems and applications. So far, this is not reflected in German regulation in this rigorous manner: BAIT point 5.6 and ZAIT point 5.6 speak of "the IT systems" (and not "all IT systems") and the "regular" review. The exception is found in VAIT para. 5.6, according to which insurance companies already have to review "critical systems ...at least annually".	Article 21 (6)
Q	Threat-oriented penetration tests	So far, threat-oriented penetration tests are known from TIBER-EU and in Germany participation in TIBER-DE is voluntary. Now threat-oriented penetration tests will become mandatory. They must be carried out for critical and important functions at least every three years, including on outsourced functions. The tests are carried out on live production systems. The competent authority must approve the scope of the penetration test in advance and also certify that it has been carried out properly after it has been performed. If internal testers are used, external testers must be involved every 3 tests.	Article 23
R	Checking the suitability of the testers	From the extensive requirements for testers, the recommendation of securing testing capacities at an early stage must be derived. The requirements of DORA are also new for the testers, so that the supply of DORA-compliant testers will probably not be able to cover the demand in Q3 2025 when DORA is applied.	Article 24
S	Use of internal testers is subject to conditions	Major hurdles before the use of internal testers due to three conditions: - They must be approved by the competent authority; - Competent authority checks for sufficient resources and avoidance of conflicts of interest throughout the planning and execution of the test; - the "threat intelligence" provider is not affiliated with the financial entity	Article 24 (1a)

No.	New field of action	Description / Conclusion	Source
T	Preparation of "Strategy for Risks from ICT Third-Party Providers", contains, among other things, contract register on ICT third-party providers	In principle, this strategy can be seen as an outsourcing strategy already familiar to the BaFin supervisory objects - in this case with a focus on "ICT third-party providers". For all new DORA supervisory objects, however, this will be a new and not easy task to fulfil. To what extent BaFin will demand this new strategy as a separate strategy or accept it as part of an existing strategy will become clear after DORA comes into force.	Article 25 (3)
U	Informing the competent authority about the planned procurement of contracts for critical or important functions	This requirement has also been known to the existing BaFin supervisory objects since the beginning of the year through the FISG, so that an adaptation to DORA should not represent an excessive effort, as it will be for new DORA supervisory objects. The subsequent information when a function is upgraded to critical or important is also known from the FISG for previous BaFin supervisory objects.	Article 25 (4)
V	Preparation of exit plans	In the draft version of DORA of 24. September 2020, the phase-out plans were still to be "sufficiently tested, where appropriate", which was sufficiently vague. In the trilogue compromise text of 23. June 2022, the phase-out plans must be comprehensive, documented and sufficiently tested and regularly reviewed in the sense of the proportionality principle under Article 3a para. 2. The new wording reduces the vagueness. Nevertheless, the "sufficient testing" of exit plans is a very big challenge for all financial entities. Example: How should a bank sufficiently test its hyperscaler?	Article 25 (9)
W	Assessment of ICT concentration risk	All financial firms must assess ICT concentration risk prior to potential outsourcing. This entirely new requirement poses a high hurdle for all financial entities. They have to consider various aspects such as "ease of substitution", "multiple contractual arrangements with the same/closely related ICT third party provider". In addition, alternatives have to be investigated and risks from subcontractors of the ICT third party providers have to be assessed. Furthermore, financial entities must also assess whether the outsourcing chain enables the supervisor to supervise the financial entities. The article consists of imponderables; only (audit) practice will show whether and how these requirements can be implemented.	Article 26
X	Essential contractual provisions	Observance of minimum contents of the contract between financial companies and ICT third party providers, among other things, termination rights must "meet the expectations of the competent authority". These "expectations of the supervisory authority" cannot be estimated	Article 27

No.	New field of action	Description / Conclusion	Source
		today. Do they differ from country to country or are they uniform across Europe?	

Author

Waldemar Grudzien is an Expert Partner at CORE and founder of the Regulation and Compliance Practice. He holds a doctorate in electrical engineering and a degree in economics. His work focuses on information security, data protection and auditing in the financial sector - keyword: §44 KWG audit. He supports clients in the development and secure operation of certifiable ISMS and PIMS.

Mail: waldemar.grudzien@core.se

Katrin Miller is a **legal expert** at CORE. She brings extensive experience from information security projects in the financial sector; in particular, she has application knowledge on the topics of information risk management, BIA (Business Impact Analysis) and PNR (Protection Needs Requirements). Ms Miller is also involved in money laundering prevention.

Mail: katrin.miller@core.se

Theresa Sporn is an Expert Fellow at CORE and holds a Bsc. in Management. During her studies, she gained work experience in consulting and then in data science at an HR tech company and supports the team at CORE with data analysis and visualisation.

Mail: theresa.sporn@core.se

Moritz Treutwein is **Transformation Manager** at CORE. His consulting focus is Banking & Capital Markets, and his expertise includes the management and implementation of business area expansions in the context of IT implementation projects, audit remediations, and the development of digital business models. He is also CORE's Information Security Officer**.**

Mail: moritz.treutwein@core.se

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zurich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC - 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633
office@core.se