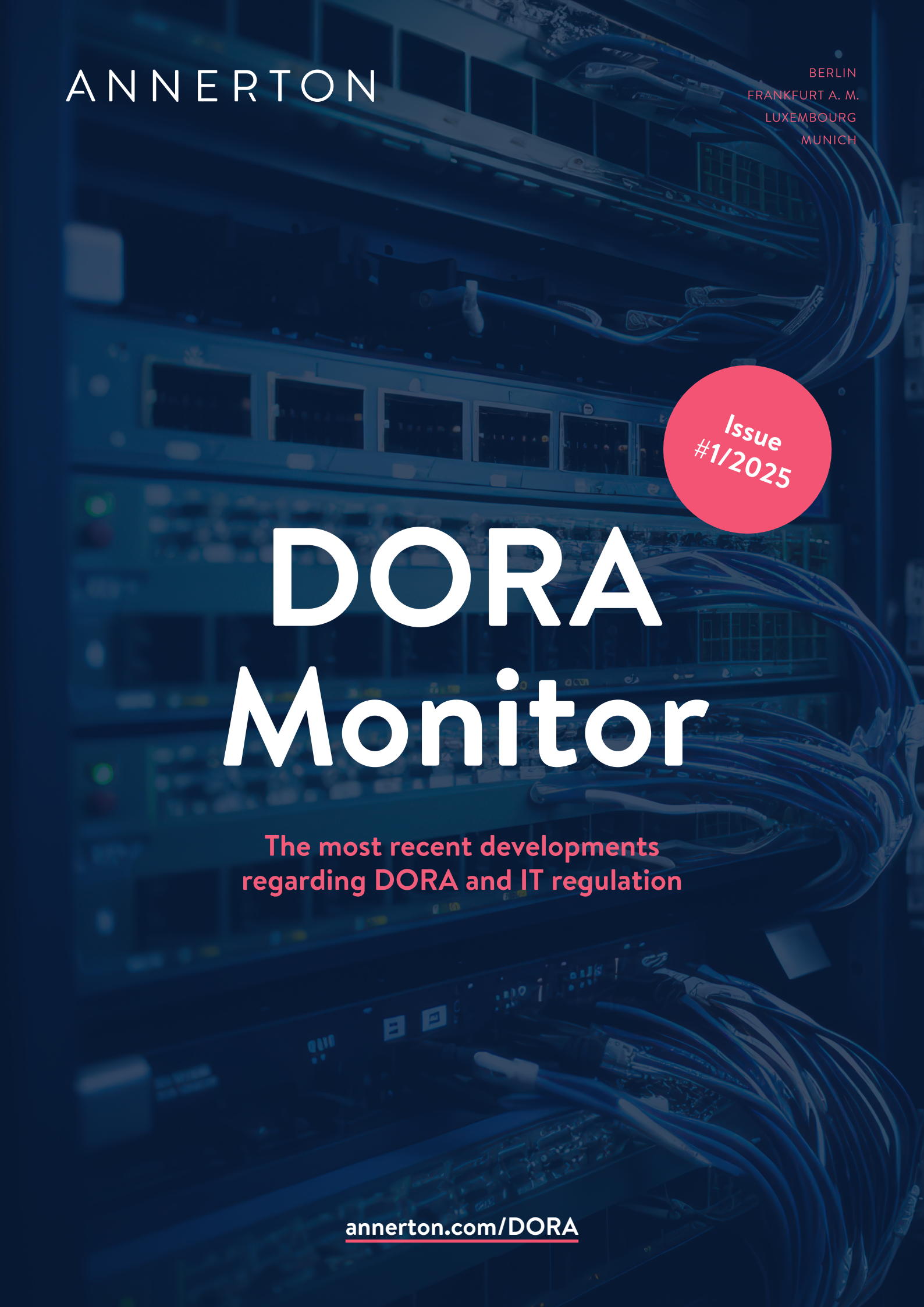
ANNERTON

BERLIN
FRANKFURT A. M.
LUXEMBOURG
MUNICH



Issue #1/2025

DORA Monitor

The most recent developments regarding DORA and IT regulation

annerton.com/DORA

Dear Readers,

With this issue, we are launching a new informational series for the financial sector: the DORA Monitor. The goal of this series is to provide you, on a regular, concise, and practice-oriented basis, with essential updates on developments related to the EU Regulation on Digital Operational Resilience in the Financial Sector (DORA), as well as on adjacent regulatory matters concerning IT requirements.

DORA constitutes not only a milestone in European regulation on digital resilience, but also a significant challenge for financial institutions regarding practical implementation – especially in the areas of ICT risk management, outsourcing (including sub-outsourcing), and reporting obligations. The regulatory requirements in these fields are currently being rapidly clarified through regulatory technical standards (RTS), guidelines, national specifications, and the first supervisory audit experiences.

In this inaugural issue, we report, among other things, on the long-awaited release of the RTS SUB, which details requirements for sub-outsourcing of ICT services supporting critical or important functions. We also shed light on the latest activities from BaFin (the German Federal Financial Supervisory Authority), particularly the updated overview of minimum contractual content, the revised FAQs concerning ICT incidents, and the direct applicability of the ESA (European Supervisory Authorities) Guidelines on ICT-related incident reporting.

A special focus of this edition is a review of the initial submission process of the DORA information register from a practitioner‘s perspective, along with first insights gained from recent DORA audits within our advisory activities. These insights reveal the specific aspects on which supervisors and auditors are already focusing – and highlight practical pitfalls that are often overlooked during implementation. Accordingly, you will receive valuable guidance for your own preparation for upcoming audits and for the effective structuring of DORA compliance.

We are pleased if our DORA Monitor becomes a reliable and valuable companion to you in the implementation of regulatory requirements. Should you have any questions, wish to discuss particular issues, or require in-depth workshops, we always remain at your disposal.

Your

Annerton Team

TABLE OF CONTENTS

Status of this issue 1/2025: 01.08.2025

THE NEW DORA RTS SUB IS NOW AVAILABLE!

On 2 July 2025, the European Commission formally adopted the regulatory technical standard (RTS) clarifying the aspects that a financial entity must determine and assess when sub-outsourcing ICT services in support of critical or important functions (so-called RTS SUB), as Delegated Regulation (EU) 2025/532. The RTS SUB sets out the specific requirements that financial institutions must fulfil when outsourcing or sub-outsourcing ICT services. These requirements must be observed whenever critical or important functions of a financial entity are supported by an ICT service. In particular, the requirements established in the RTS SUB are relevant for the risk assessment and the management of ICT sub-service providers.

In February 2025, the Commission initially rejected the adoption of the original draft of the RTS SUB. The draft presented by the European Supervisory Authorities (ESAs) in July 2024 contained requirements relating to the "conditions for sub-outsourcing within the chain of ICT subcontractors," which, in the Commission's view, exceeded the mandate established in Article 30(5), fourth subparagraph of DORA. The Commission argued that these requirements were not sufficiently linked to the conditions for sub-outsourcing and thus went beyond the scope of the mandate. Accordingly, the ESAs were requested to delete Article 5 as well as the corresponding Recital 5 from the original draft of the RTS SUB. The ESAs complied with this request and, on 24 March 2025, submitted an updated draft of the RTS SUB, which has now been adopted and published by the Commission.

The RTS SUB will become effective on 22 July 2025.

Practical significance of the new RTS SUB for financial institutions:

The new RTS SUB specifies and extends the requirements laid down in DORA regarding the use of ICT services by financial institutions. Its focus is on the aspects that a financial institution must consider in the context of further or sub-outsourcing of ICT services when such services support critical or important functions. Essentially, the significance for financial institutions can be summarized as follows:

- **Clear sub-outsourcing processes**
  The RTS SUB sets out detailed criteria on how financial institutions must structure and control sub-outsourcing. In particular, clear processes must be established to ensure that sub-service providers meet the same security, data protection, and compliance requirements as the original service provider.

- **Diligence obligations and risk assessment**
  Financial institutions may only outsource an ICT service to a third-party service provider under the requirements of the RTS DORA if the provider can ensure controlled and trans-

parent sub-outsourcing of ICT services to support critical or important functions at the financial institution and meets all regulatory requirements. With the RTS SUB, financial institutions are now subject to stricter requirements on how they must identify, assess, and manage the risks associated with sub-outsourcing (in support of critical or important functions). This concerns a wide range of risks (e.g., system failures) as defined in Article 3 (1) (a)–(j) RTS SUB. The risk assessment must consider, inter alia:

- the ability of the main service provider to identify the entire chain of sub-service providers to notify and inform the financial institution thereof and to provide the financial institution with all necessary information regarding the sub-service providers used.
- the assessment of the operational, financial and security-related performance capability of potential subcontractors.
- the assurance that the financial institution and the authorities are granted full access, audit, and information rights along the subcontractor chain.
- sufficient capabilities, expertise, and adequate financial, human, and technical resources at the main service provider to monitor ICT risks at the subcontractor level.
- the assessment by the financial institution of location risks in relation to potential sub-service providers/sub-services, ICT concentration risks, and the impact that a potential failure of a subcontractor providing ICT services to support critical or important functions, or a material part thereof, may have on the digital operational resilience and the financial soundness of the financial institution.

Financial institutions must therefore enhance their risk management with respect to ICT services supporting critical or important functions. Regular reassessments and updates of risk analyses must also be implemented, particularly in the event of changes to the supported business functions, including ICT threats, ICT concentration risks, and geopolitical risks.

- **Requirements for the contract with the main service provider**
  The RTS SUB sets out a wide range of requirements regarding sub-outsourcing and the contractual arrangements in this respect between the financial institution and the ICT third-party service provider supporting critical or important functions, or material parts thereof. Among other things, it is clarified that
  - the main service provider remains responsible even in the case of sub-outsourcing.
  - the main service provider is required to monitor the sub-service providers and to ensure the fulfilment of the contractual obligations towards the financial institution. This includes specific reporting obligations to the financial institution.
  - the main service provider is required to conduct a risk assessment regarding the sub-service providers/sub services used and the location of data processing or storage by the subcontractor engaged.
  - the main service provider must ensure the continuity of ICT services supporting critical or important functions along the entire chain of subcontractors if an ICT subcontractor fails to fulfil its contractual obligations.

- the financial institution must contractually secure various direct rights of intervention (in particular regarding compliance with ICT security standards, business continuity plans and access/audit rights).

Furthermore, Article 6 RST SUB stipulates specific termination rights that must be contractually agreed between the financial institution and the main service provider in connection with sub-outsourcing when critical or important functions or parts thereof are supported at the financial institution.

- **Handling of material changes**
  The new RST SUB requires financial institutions to include in their contracts with the main service provider that the ICT third-party service provider must notify the financial institution in advance of any intended material changes to existing subcontractor agreements relating to ICT services for critical or important functions. This is intended to enable the financial institution to assess in a timely manner the impact on its risk position and the performance capability of the main service provider. The contract must provide for an appropriate period for notification and review. Without explicit consent or explicit non-objection, the service provider may not implement changes. If the financial institution determines that the proposed changes exceed its risk tolerance, it is obliged to notify this within the specified period, to reject change and, if applicable, to request adjustments.

BAFIN: UPDATES ON DORA

In recent weeks, the BaFin has published a range of updates on DORA on its website https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html. In the following, we address updates that are of high practical significance:

1. Update of the overview of the minimum contractual contents under DORA

Most recently, on 24 June 2025, BaFin once again updated the overview of the minimum contractual contents under DORA and published the current version on its website.

With this overview, BaFin provides the financial institutions affected by DORA with an Excel overview specifying which minimum requirements must be included in contracts between them and their ICT third-party service providers. The basis is formed by Articles 28-30 DORA as well as the corresponding RTS TPPol (Commission Delegated Regulation 2024/1773 of 13 March 2024 – Regulatory Technical Standards specifying the detailed content of the policy for contractual arrangements on the use of ICT services supporting critical important functions provided by ICT third-party service providers) and RTS SUB.

What is new?

The current version takes the following aspects into account:

- **Obligations related to sub-outsourcing chains:**
  The requirements from the new RTS SUB, in particular regarding contractual arrangements in the case of subcontracting by ICT service providers, are already included in the table of minimum requirements. BaFin has worked on this basis using the draft of the new RTS SUB, but compared to the now adopted Delegated Regulation 2025/532 (new RTS SUB), there are no substantive differences from the draft of the new RTS SUB.

  According to Article 3 (1) (b) RTS SUB, the financial entity is still required, prior to concluding the contract, to verify whether the ICT service provider is able to identify and report all sub-service providers in a sub-outsourcing chain and to provide all relevant information. In addition, during the contractual relationship, the ICT service provider must ensure the continuity of the ICT service supporting critical or important functions throughout the entire sub-outsourcing chain (Article 4 (1) (g) RTS SUB) and report any material changes in the sub-outsourcing arrangements (Article 4 (1) (k) RTS SUB).

However, the obligation to include contractual provisions with the sub-service provider that enable the financial entity to effectively monitor the services has been removed. The obligation to agree on contractual provisions for the identification of risks associated with long sub-outsourcing chains has been removed as well.

Pursuant to Article 5 (1) RTS SUB, a provision must now be included requiring the ICT third-party service provider to inform the financial entity in a timely manner of any intended material changes to its subcontracting arrangements, so that the financial entity can assess the impact on the risks to which it is or could be exposed and determine whether such material changes could affect the ICT third-party service provider's ability to fulfil its contractual obligations to the financial entity. A corresponding notification period must be agreed, during which the financial entity can approve or reject the change. The changes may only be implemented once the financial entity has approved them or has not rejected them (Article 5 (3) RTS SUB).

- **Notes on specific case groups:**
  BaFin has newly included clarifications and notes for financial entities falling under the simplified risk management framework pursuant to Article 16 (1) DORA, as well as for micro-enterprises pursuant to Article 3 (60) DORA. This is particularly relevant because the RTS TPPol pursuant to Article 28 (2) DORA does not apply to these entities. For micro-enterprises, Article 30 (3) DORA provides that an independent third-party appointed by the ICT third-party service provider may also be engaged to exercise access, inspection and audit rights. The financial entity that is a micro-enterprise may also request information and assurances regarding the services of the ICT third-party service provider at any time.

You can find the current overview and further information on the application of the new requirements on the BaFin website at the following link:
https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/dl_2024_08_05_Mindestvertragsinhalte_DORA_DE_EN.html

2. FAQs on ICT incident updated

BaFin updated its questions and answers on the handling, classification and reporting of ICT-related incidents on 13 May 2025. In particular, BaFin has incorporated the requirements of Delegated Regulation 2025/301 (RTS specifying the content and deadlines for initial, intermediate and final reports of major ICT-related incidents, as well as the content of voluntary reports of significant cyber threats) into its FAQs and has, for example, highlighted that an exemption regarding reporting deadlines on weekends and public holidays applies pursuant to Article 5 (4) RTS Reporting, according to which an incident report (initial, intermediate or final) may be submitted by 12:00 noon on the next working day. However, this only applies to financial entities that are neither credit institutions, central counterparties, trading venue operators nor other financial entities classified as essential or important entities or critical infrastructures under national laws implementing Article 3 NIS2.

3. ESA-Guidelines on ICT incident directly applicable

In its current guidance on the handling, classification and reporting of ICT-related incidents, BaFin has explicitly clarified that the Joint Guidelines of the European Supervisory Authorities (ESA) of 5 June 2024 (JC/GL/2024/34) on the estimation of aggregated annual costs and losses caused by major ICT incidents are directly applicable.

Financial sector entities must therefore comply with the estimation methods set out in Title III of the ESA Guidelines for their reporting on ICT incidents with immediate effect. The cost estimation is then carried out by aggregating the annual costs and losses for all ICT-related incidents that occur within a specified reference year. The reference year may be either the calendar year or the financial year of the entity. For each incident, gross costs and losses as well as any financial recoveries must be identified and aggregated. The estimates should be based on costs, losses and financial recoveries reported in the annual financial statements such as the profit and loss account or, where applicable, in the reports tot he supervisory authority for the relevant reference year. In their estimations, financial entities should also include accounting provisions reported in their annual financial statements, such as the profit and loss account for the relevant reference year.

REVIEW: INITIAL SUBMISSION OF THE DORA INFORMATION REGISTER

For the first time, all financial entities were required to submit their DORA information register to BaFin via the MVP reporting portal by 28 April 2025. The original, much earlier deadline of 11 April 2025 could not be met due to significant technical and organizational issues on BaFin‘s side. As a result, the submission deadline was extended and a testing phase was established from 14 to 28 April 2025, during which institutions received feedback and error messages on their submissions and were able to make corrections without sanctions.

From a practical perspective, the initial submission was marked by numerous errors and ambiguities. In particular, the technical requirements for the information register, which must be based on the complex and EU-wide harmonized specifications of the ESAs, resulted in the templates provided by BaFin being prone to errors and having limited practical usability. At the time of the initial reporting obligation, only insufficient and difficult-to-understand guidance was available, so that many financial entities had considerable difficulties in implementing the requirements for the information register and, to this day, often cannot be certain whether their submission meets the supervisory requirements. Communication regarding format and data specifications also proved to need clarification. Overall, the process was marked by uncertainties and was far from smooth assessed from a practical perspective.

Only gradually did BaFin publish additional completion notes and explanations, which have increasingly contributed to clarifying the required format and necessary content. A final assessment and genuine practical insights will probably only be possible once the European Supervisory Authorities (ESAs) have completed the initial evaluation of the submitted information registers and published any feedback or clarifications. Until then, many institutions still face significant legal and implementation uncertainty.

INITIAL FINDINGS FROM DORA AUDITS

BaFin and Bundesbank have begun to obtain an initial overview of the implementation status of DORA through mandated IT audits. Initial reports from DORA audits already conducted paint a consistent picture of the existing challenges in the practical implementation of DORA.

- ICT risk management as a key focus: Initial practical insights from conducted DORA audits indicate that supervisory authorities are also placing a strong focus on establishing transparent and practical processes for ICT risk management. Initial experience already shows that established internal control mechanisms, particularly in the areas of continuous monitoring, contingency planning and outsourcing management, are central to the audits. Observations from the initial audits also indicate that supervisory authorities place particular emphasis on the quality of risk analysis, the timeliness of inventories and clear internal assignment of responsibilities.

- No individualization: It is noteworthy that many institutions have so far formally incorporated the DORA requirements into their internal policies and processes – often by almost adopting the legal provisions – but have not sufficiently adapted them to the individual circumstances and specific risks of their own institution. This is regularly raised as a critical point by the auditors and assessed as a lack of implementation depth.

- Lack of definitions: Another problem area concerns the definition and delineation of key terms as well as their consistent application in the processes. Terms such as „anomaly“ or „ICT incident“ are often not clearly distinguished from each other, which leads to uncertainties regarding categorization, reporting obligations and further handling of incidents within the institution.

- Roles, responsibilities and accountabilities are often unclear or not sufficiently clearly assigned, leading to significant organizational and management deficiencies.

- technical audit standard: From a technical perspective, auditors apparently place significant emphasis on the BSI IT standard (BSI IT-Grundschutz), so that the requirements in the areas of information security, risk management and technical organization are closely aligned with this standard. In particular, processes and measures in the areas of ICT security, governance and documentation are analysed based on the protection objectives established by the BSI.

- Classification of ICT assets: The classification of „critical or important functions“ within the meaning of DORA and their assignment to all existing ICT assets and ICT service providers

also proves to be challenging in practice. There i soften a lack of systematic and comprehensive application of the requirements, which complicates risk management and compliance with supervisory requirements.

- Contracts with ICT service providers: Significant deficiencies are also observed in contracts with ICT service providers. Many contracts do not meet the minimum requirements of Article 30 (2) and (3) DORA, and there is still little clarity in practice as to which specific services are to be classified as ICT services under DORA. The requirements for dealing with full-service solutions, which are often used in practice and partly comprise ICT services and partly non-IT services, are unclear. Also here, there are still significant uncertainties and, in some cases, considerable gaps in practice.

Individual results and feedback from already completed audits have not yet been publicly documented, partly due to the sensitivity of the subject and the relative novelty of the regulation. However, legal practice is already observing that companies are proactively making strategic and operational adjustments to their ICT governance to further meet the regulatory requirements of DORA.

In summary, the DORA audits conducted so far show that considerable effort is required in the areas of individual adaptation, definition of terms, and institution-specific structuring of documentation. In their audits, the supervisory authorities do not only focus on the formal adoption of DORA requirements, but in particular on their practical and risk-adequate implementation for each institution—and on ensuring that terms, responsibilities, and processes are clearly, transparently, and consistently defined.

For practical purposes, it would be extremely helpful if the supervisory authorities were to specify their expectations regarding the interpretation and implementation of the DORA requirements in clarifying publications, analogous to the former xAIT. Such clarification would provide financial entities with more reliable guidance for the practical implementation of regulatory requirements and effectively reduce uncertainties in the audit process. We assume that the insights gained from the DORA audits already conducted and those upcoming will be evaluated by the supervisory authorities and communicated in the form of appropriate publications. This would make best practice approaches, typical challenges, and supervisory priorities for the industry transparent and further harmonize and facilitate the implementation of DORA requirements. With the Guidance on the implementation of DORA in ICT risk management and ICT third-party risk management as well as its supervisory notice on outsourcing to cloud providers BaFin has already begun to implement this accordingly.

ABOUT THE AUTHORS

Josefine Spengler

LAWYER
CERTIFIED LAWYER FOR INFORMATION TECHNOLOGY LAW (IT-LAW)
COUNSEL

T +49 30 863 21 88-26
E JSpengler@annerton.com
Full profile

Peter Frey

LAWYER
PARTNER

T +49 89 306 683 -215
E PFrey@annerton.com
Full Profile

Contact us at
DORA@annerton.com