ECUC´s POSITIONS ON DORA

As a trusted advisor and catalyst the European Cloud User Coalition (ECUC) fosters a secure and effective usage of Public Cloud Computing in the European Financial Services Industry. The ECUC currently represents 32 European Financial Institutions.

For more information visit: https://ecuc.group
Follow us on: https://de.linkedin.com/company/ecuc-european-cloud-user-coalition
Contact: info@ecuc.group

Introduction

DORA, the Digital Operation Resilience Act - Regulation (EU) 2022/2554, aims to increase the resilience of the European financial sector by unifying and simplifying compliance with existing regulation on risk management and security of information and communication technology (ICT). The Regulation entered into force on 16th January 2023 and applies from the 17th of January 2025.

DORA includes several supporting technical acts (Regulatory Technical Standards RTS/Implementing Technical Standards ITS), which contain more practical aspects related to governance and reporting requirements. Public consultation on these supporting acts have recently been held and the official publication of these documents is expected in the second half of 2024 – which creates a challenge for all institutions that are required to be compliant with the regulation by January 2025.

The ECUC welcomes DORA and its ambitions to ensure that necessary safeguards are in place to mitigate growing cyber-attacks and other ICT-risks to increase financial organizations digital resilience. Even though DORA in the short term will have a high impact on financial institutions ability to use cloud computing. We also appreciate the harmonization with other legal standards and frameworks where appropriate and look forward to and appreciate the audit of designated critical ICT third-party service providers.

General feedback on DORA

Taking this into account and not to restrict the use of cloud computing further we have the following recommendations:

- Article 4 introduces the principles of proportionality for a practice-oriented implementation of DORA. These should be used for ICT-risk management, ICT-related incident management and resilience testing. We believe that competent authorities should also take the principles into account when reviewing ICT risk management.
- As the requirements resulting out of DORA are very complex and deadlines are very tight, it will be difficult for European Financial Institutions to implement them accordingly to achieve compliance before all final supporting legislative texts are published in the Official Journal (e.g. a lot of processes and contracts must be adjusted).

- This not only leads to a high level of legal insecurity but also to a situation where a Financial Institution implements needs that should be revisited at a later point in time when these requirements are formalized i.e. the lack of formalization can lead to a higher level of digital operational risks than intended on DORA Level 1 texts. To ensure that resources are allocated to really enhancing digital operational resilience and avoid potential caveats, we recommend that the implementation deadline would be postponed to the 17th of January 2028 in dialogue with supervisors.

Draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework under Article 15 and 16(3) of Regulation (EU) 2022/2554

The ECUC provided feedback to European Supervisory Authorities´ consultation on the draft RTS on ICT-Risk Management Framework. With the provision of the final draft, clarifications and improvements have been introduced in various areas of the RTS. The clarification of proportionality principles, ICT project and change management, encryption and cryptography, risk-based approach, the reduction of overlap with other requirements and omission on details of security awareness programs and governance are especially welcomed.

On network security, we acknowledge and appreciate the change in the final version with regards to documentation of networks and data flows which earlier required mapping of them. However, the requirement to review ICT systems supporting critical or important functions at least every 6-months causes particular concern (draft RTS Article 13(1)(h)). For larger organizations, given the multitude of systems in operation, this will in practice result in organizations conducting continuous, rolling reviews.

The ECUC positions and possible solutions to relevant topics can be found in the specific chapters of the next version of the ECUC Position Paper and related ECUC Checklist, which will be published in autumn.

Draft RTS to specify the policy on ICT services supporting critical or important functions under Article 28(2) Regulation (EU) 2022/2554

With reference to draft RTS Article 3(3), stating "*a methodology for determining which ICT services support critical or important functions*", an alternative proposal would be to refer to the ICT services supporting critical/important functions as outlined within the Register of Information. We appreciate that DORA does not make any requirements between having a multi-vendor strategy or not hence the requirements are only needed if applicable.

While termination of contract is and will continue to be the last resort, we believe that any additional burden for FIs to terminate their contracts with CSPs are counterproductive. Further it is important to ensure that current contracts are not required to be updated until they are terminated with a maximum term of 10 years.

Draft RTS on subcontracting ICT services supporting Critical and Important Functions under Article 30(5) of Regulation (EU) 2022/2554

DORA's ambition to give the financial sector greater control over the sub-outsourcing chain is a noble goal, and highly relevant in the context of cloud outsourcing. However, there is a large gap between reality and the envisaged objectives.

According to the ECUC, to properly determine the relationship between cloud user and Cloud Service Provider, and avoid discussions, we welcome a more detailed legislation, including extensive explanation of the elements that should be taken into account when deciding upon the acceptability of subcontracting.

Without withholding the financial entity's final responsibility, ECUC is also in favour that a Cloud Service Provider is allowed to give assurance that its sub outsourcing chain has adequate abilities, expertise, resources, controls, etc. Assurance on which the Cloud Service Provider is only required to perform marginal checks.

DORA Harmonization with industry standards

DORA also aims to harmonize with other industry standards and regulations, this is something that we appreciate, however in some areas it may require further clarification. Below some areas where harmonization is evident:

- Threat led penetration testing has been aligned with most of the requirements from TIBER EU framework, we also noticed there have been enhancements or improvements to the requirements provided in DORA such as purple team, allowing internal testers for certain period. A question we have is what the purpose of TIBER will be once DORA is implemented?
- The policy on use of ICT services is incorporating requirements from EBA guidelines on outsourcing such as due diligence, risk assessments and exit strategy. However, the data points on register of information for third parties and sub-contractors are way too detailed and requires some practicality in terms of implementation.
- The requirements on incident reporting are extracted from PSD2 requirements and further enhanced by removing the complications of working days to submit interim and final report. However, with the new DORA timelines and regulatory reporting requirements it is not explicitly specified if we need to continue reporting based on other regulatory requirements. It is prudent to unify ICT-related incident reporting and address overlapping reporting requirements.
- For network and information security, DORA is considered Lex-specialis, the provisions of DORA relating to ICT risk management (Article 6 et seq.), management of ICT-related incidents and, in particular, major ICT-related incident reporting (Article 17 et seq.), as well as on digital operational resilience testing (Art 24 et seq.), information-sharing arrangements (Article 45) and ICT third-party risk (Article 28 et seq.) shall apply instead of those provided for in the NIS 2 Directive. The DORA precedence holds true also for Critical Entities Directive (CER).

Certification Schemes

We would encourage ESAs to establish standardized certification schemes to facilitate third party assurance. For instance, financial entities could rely on standard certification schemes such as ISO 27001, SOC II, EU Cloud Certification Scheme and other internationally accepted standards. This should not limit the use of using third parties which do not have certifications, in which case the financial entity should take appropriate measures to ensure assurance.

DORA Section II Oversight Framework of Critical ICT third-party service providers (CTTPs) and accompanying RTSs

The requirements for direct oversight of designated CTTPs providers described under DORA Section II and the associated RTS on harmonisation of oversight activities and joint draft guidelines on oversight cooperation leave potential for customers, ICT third-party service providers (ICT TPPs) and supervisors unused. The ECUC encourages the following items to be considered for future adjustments and enhancements.

ECUC would appreciate if the ESAs could provide audit catalogues and audit results to all (contractual) parties to achieve full transparency and to avoid multiple audits of the same subject areas, which is not conducive to safety.

Alternatively, the ECUC proposes that the monitored CTTPs make the full results available to their clients in order to provide transparency on the scope and outcome of the supervision. In particular, since serious or unresolved findings are intended for further mitigation, the proposed practice would also - in a positive sense - create transparency and certainty about the proper and DORA-compliant management by CTTPs.

Technical Advice on the Criteria for Critical ICT Third-Party Service Providers (CTTPs) and Fees for Oversight Framework under Articles 31 and 43 of Regulation (EU) 2022/2554

Regarding the European Commission´s delegated acts specifying the criteria for designation of ICT TPPs as critical for financial entities, the ECUC maintains that:

- The criteria do not take concentration risk on a member state level into account (a provider can be critical on a national level but according to the proposed criteria and calculation method would not be considered critical on the EU level).
- The criteria do not consider what type of service from ICT TPPs (ICT service versus e.g. the provision of market data).
- The criteria to assess systematic impact of the ICT TPP is based on a number of financial entities serviced but does not take into account the size of financial entities (e.g. by number of customers/size of the market).
- The criteria to determine criticality or importance of the function could be divided to distinguish between criticality and the number of very critical functions.
- The criteria to estimate the degree of substitutability should have been based on the total assets instead of number of financial entities of a category of financial entities.

Reporting of register of information will be critical to designate CTTPs, as implementation is needed by January 17th 2025, to provide this as an input for the ESAs to analyse all the ICT TPPs used by Financial Institutions based on size, finances and footprint of ICT TPPs within the financial sector. This will provide insight into concentration risk on Cloud Service Providers where they might be assigned as CTTPs.

DORA introduces the oversight fees calculated based on the turnover of a CTTPs which are the revenues generated in the European Union from the provision of defined ICT services (Article 28(9) of Regulation (EU) 2022/2554).

We propose an effort-based approach that explicitly promotes the transparency of service providers in auditing and creates positive incentives. Effort could be reflected e.g. like this:

Effort-related coefficient in year (n) = hours of ESA oversight performance for a CTTP concerned in year (n-1) / hours of all ESA oversight performance for all critical ICT third-party services in year (n-1).

Challenges on DORA

The ECUC foresees several challenges implementing DORA such as:

- First and foremost, the timelines to implement are considerably shorter for a regulation that has several levels of details that are yet to be finalized. For instance, the second batch of RTS would be finalized and delegated by September 2024, however it is expected to be effective by 17th January 2025. As proposed earlier, we would like the deadlines to be extended to cater for quality and a legally safe implementation.
- Although there is certain level of harmonization with other frameworks, the definitions provided in DORA are very broad for ICT services and thus increasing the scope of activities to be performed by multiple folds. In certain cases, the definitions are too vague or not provided leaving room for interpretation.
- DORA emphasises time and again on harmonizing with other standards and frameworks like TIBER-EU framework, EBA guidelines on outsourcing, PSD2, where we see multiple overlaps however there is no clarity to avoid double reporting or completely stop activities on other frameworks once DORA is adopted.
- Register of information for ICT TPPs and sub-contractors are way too detailed and requested to be available by 17th January 2025 to aid the designation of CTTPs, however the register itself is not yet finalized and it seems practically challenging to have the register in such short timelines. Also, the fact that the register of sub-contractors is completely a new addition.

Visit our website https://ecuc.group for ECUC Position Paper v.2.2 covering all cloud related aspects.

32 European FIs are members of the ECUC. Amongst others these are: ABN AMRO Bank N.V., Allied Irish Banks, Bank of Ireland, BAWAG Group, BayernLB, Belfius Bank, Berenberg, Commerzbank AG, Creditplus Bank AG, Deutsche Börse AG, Deutsche Kreditbank AG, Deutsche Pfandbriefbank AG, DNB Bank ASA, Erste Group Bank AG, Euroclear, Gothaer Finanzholding AG, ING Groep N.V., KBC Bank NV, Landesbank Saar, Nordea Bank Abp, OP Financial Group, Permanent TSB, Raiffeisen Bank International, Swedbank AB, Traton Financial Services AB and UniCredit S.p.A.