Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Comments

GBIC position paper on the European Commission legislative proposal „regulation on digital operational resilience for the financial sector" (DORA) of 24.September 2020

Contact:

Berit Schimm

Telephone: +49 30 2021-2111

Telefax: +49 30 2021-19 2100

E-mail: b.schimm@bvr.de

Berlin, 14. December 2020

Coordinator:
National Association of German
Cooperative Banks
Schellingstraße 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Telefon: +49 30 2021-0

Summary of GBIC Comments

- We explicitly welcome a harmonisation of the various European regulatory approaches in the field of cybersecurity.
- The current legislative proposal goes far beyond the harmonisation approach initially planned by the European Commission. Additional detailed requirements lead to additional costs without actually improving cyber-resilience.
- Lack of proportionality: Exceptions only for so-called micro-enterprises are not sufficient.
- Major incident reporting must be combined in a single procedure that includes PSD2- and NIS incident reporting.
- The requirements for the management of ICT Third Party Risk should distinguish whether or not the ICT service supports critical / essential functions.
- A multi-vendor approach is neither necessary nor purposeful to address concentration or lock-in risks.
- Facilitation of outsourcing by groups and institutions which are members of an institutional protection scheme, as provided for in the EBA guidelines on outsourcing arrangements, should also be applied to the management of ICT services provided by third parties.
- A supervisory framework for critical ICT service providers operating across Europe should be combined with easier monitoring by financial institutions.
- In supervising critical TPPs, national legal frameworks and established national structures must be taken into account.

In Detail:

DORA is a step towards harmonisation, which the industry sorely needs. The implementation of EU-wide security standards and harmonised tests and uniform reporting structures is crucial if we are to deepen harmonisation of the single European digital market. Removing national inconsistencies in implementing security standards and in supervisory practices will be key to fostering EU-wide innovation.

However, the current legislative proposal goes far beyond the harmonisation approach initially planned by the European Commission. Exceptions are only provided for so-called "microenterprises". Its definition does not include banks, due to the low balance sheet total limit and/or the usual size of the workforce. Thus, the proportionality principle is not sufficiently applied.

The current regulatory standards of EBA and the German National Federal Financial Supervisory Authority follow a proportionality approach, particularly with regard to the risk and complexity of institutions. The principle-based requirements of these guidelines currently leave scope of action with regards to their implementation. However, the additional detailed requirements in the legislative proposal lead to (bureaucratic) increasing efforts (e.g. in documentation) and additional costs without actually improving cyber-resilience. The Regulatory Technical Standards (RTS) of the ESAs which are foreseen by the current proposal are expected to result in an even greater density and depth of regulation. There should be no legal definition of methods via RTS, as short-term adaptability of methods and practices is required, especially in the field of IT security.

Existing requirements of the NIS- and PSD2 Directives would overlap with the requirements presented in the current proposal, so that an adaptation of these Directives would also be necessary if points were to be incorporated in a new Regulation in their present form. On the other hand, the planned harmonisation of the reporting system for security incidents

should be emphasized positively. Of course, major incident reporting must be combined in a single procedure that includes PSD2- and NIS incident reporting.

The requirements for the management of ICT Third Party Risk should distinguish whether or not the ICT supports critical / essential functions. The provisions on termination of the contract appear to be absolute and go beyond the requirements of the currently implemented EBA guidelines. In particular, the requirements for financial institutions to terminate contractual relationships in case of breaches of contractual agreements - without any materiality limit - appears to be a disproportionate interference with contractual freedom. In addition, a multi-vendor approach is neither necessary nor purposeful to address concentration or lock-in risks. Depending on its design, a mandatory multi-vendor strategy bears the risk that in particular small companies may not be able to use ICT service providers.

As a general rule, the facilitation of outsourcing by groups and institutions which are members of an institutional protection scheme, as provided for in the EBA guidelines on outsourcing arrangements, should also be applied to the management of ICT services provided by third parties.

We also welcome in principle the idea of a new supervisory framework for critical ICT service providers operating across Europe. However, this should be combined with easier monitoring by financial institutions and the use of these service providers should not be made more difficult by restrictive requirements. The focus should be particularly on those international ICT service providers for which the enforceability of audits at the level of the individual financial institution cannot be sufficiently guaranteed. In supervising critical TPPs, national legal frameworks and established national structures must be taken into account.

As a general rule, the Regulation should have a sufficient transposition period of 36 months after entry into force (see Article 56, which, with two exceptions, only refers to a period of 12 months after entry into force).