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

## Digital Finance Package of the European Commission – legislative proposal: „proposal for a regulation on digital operational resilience for the financial sector 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, 3. November 2020

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

Comments: Digital Finance Package of the European Commission – legislative proposal: „proposal for a regulation on digital operational resilience for the financial sector of 24.September 2020

## General assessment

In principle, we welcome a harmonisation of the various European regulatory approaches in the field of cybersecurity.

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". However, 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 (BaFin) follow a proportionality approach, particularly with regard to the risk and complexity of institutions. In addition, ESAs guidelines, as opposed to a directly applicable EU regulation, allow national supervisory authorities to take account of national particularities. The principle-based requirements of these guidelines currently leave scope of action with regards to their implementation. There is no need for further legal regulations.

However, the individual provisions contained in the legislative proposal create new regulations, some of which are inconsistent with existing supervisory requirements.

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. 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 more restrictive requirements. We therefore see a need to closely examine in terms of necessity and purposefulness the proposed requirements in this chapter, but also in the chapter on ICT third-party risk management. GBIC is of the opinion that 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 the case of major ICT service providers operating predominantly at national level, audits should be carried out by national supervisory authorities, as they have a thorough knowledge of national circumstances.

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).

## The chapters in detail

### Chapter II ICT risk management

#### Section I Governance and Organisation

Too many tasks are directly assigned to the management. Within the scope of its final responsibility, the management must, for example, define risk appetite, but does not have to determine all the details itself, carry out monitoring activities and conduct regular reviews.

The requirements are written in a way that do not allow for a proportional risk-oriented interpretation.

Example:

Paragraph 3. calls for the designation of a central role for monitoring ICT service providers, even for small, less complex institutions (except for "microenterprises" cf. general assessment above).

Comments: Digital Finance Package of the European Commission – legislative proposal: „proposal for a regulation on digital operational resilience for the financial sector of 24.September 2020

## Section II

Many requirements are already known from the german national banking supervisory requirements and from the EBA guidelines on ICT and security risk management. These requirements should ESAs' guidelines, which should be harmonised accordingly. Legislation should establish the necessary framework for this.

Even though Chapter 1 is preceded by a general declaration of intent for proportional application, the requirements in this chapter nevertheless represent minimum requirements for basically all financial institutions. Again, exceptions are only provided for "microenterprises". While the current EBA guidelines will be incorporated into the Regulation and extended by additional rules, the envisaged Regulatory Technical Standards (RTS) of the ESAs would significantly expand the set of rules (cf. Article 14). The proposal thus goes far beyond a harmonisation objective, while at the same time limiting the scope of action. New RTS under Article 14 should not prescribe new methods, but should continue to be based on the application of current standards. This is particularly advantageous as common standards are continuously being developed.

Examples of requirements of the present draft that go beyond the requirements of the EBA guidelines

Examples:

- Article 5, paragraph 10: Approval of competent authorities required if financial undertakings delegate the tasks of verifying compliance with the requirements for ICT risk management to third parties.
- Article 7, paragraph 1: At least an annual review of the classification of information assets and all relevant documentation. A regular review which allows for a procedure graded according to risk should be possible, analogous to the existing rules.
- Article 7, paragraph 7: Annual ICT risk assessments covering all existing ICT systems represent a considerable effort. A risk-oriented approach should be chosen in order to allow a graduated procedure.
- Article 9, paragraph 2: Obligation for an "automatic alert", i.e. an automated SIEM system thus becomes mandatory for all financial institutions (contrary to the proportionality approach)
- Article 10, para. 2: Extensive detailed BCM requirements, which go beyond the requirements of the EBA guidelines. Theses rules should be principle-based and not regulate all details by law.
- Article 10, paragraph 9: Costs and losses cannot be directly allocated or calculated for every (security) incident. Reporting should be avoided.
- Articles 10-12 as well as Chapter III contain (further) requirements for dealing with ICT incidents.
- Article 11, paragraph 5: IT service providers of CSDs are required to provide a redundant operating environment, irrespective of the risk assessment of IT service providers. This requirement is not risk-adequate.
- Article 11, paragraph 6: An impact analysis is required to determine the recovery time for each function. This should be limited to the business critical functions (after a business impact analysis has been carried out).
- Article 12, paragraph 2: Dedicated reporting of implemented changes to the Business Continuity Policy to the supervisory authorities should be avoided.
- Article 13, paragraph 3: Coordinated communication in the case of ICT incidents is already carried out by different bodies according to their function (operational, crisis communication, press officer, etc.), a separate communication officer in the case of ICT incidents should not be required.

Comments: Digital Finance Package of the European Commission – legislative proposal: „proposal for a regulation on digital operational resilience for the financial sector of 24.September 2020

## Chapter III ICT-related Incidents

The requirements in Article 15 of this chapter are partially duplicated by the requirements in Articles 12 and 13 of Chapter II.However, they appear comparatively more appropriate with regards to their level of detail.

We welcome the standardisation of incident reporting in chapters 16 and 17. When introducing materiality thresholds for incident reporting in form of ESAs RTS, excessively rigid thresholds, e.g. absolute values, should be avoided. Alternatively, we recommend applying materiality to their own scope, impact grid and critical service profile.

The existing requirements for incident reporting, e.g. from PSD2 and the NIS Directive, shall be taken into account in the standardisation of reporting and shall be completely covered by the new reporting.

The evaluation for a single EU Hub for major ICT-related incident reporting by financial entities should take into account the risk that this could create a single point of compromise which could make attackers covetous.

## Chapter IV Digital operational resilience testing

In Germany, the general requirements for all institutions are already being taken up in the German banking supervisory requirements for IT (german BAIT) amendment as part of the implementation of the EBA guideline.

The legislative proposal goes beyond that in parts:

- Article 21, paragraph 5 explicitly requires institutions to use internal validation methods that fully address all vulnerabilities and gaps. Appropriate evidence from ICT service providers should also be recognised.
- Article 21, paragraph 6 requires in general at least annual testing of all critical ICT systems.
- Article 22, para. 1 requires the use of the full range of test methods, while the EBA guidelines allow for differentiation according to rotation, type and scope. The review should be based in particular on the protection requirements and the potential vulnerability of the IT system.

On Article 23 "Advanced testing":

Threat led penetration tests (TLPT) are a good building block for effective cybersecurity protection and, depending on the criticality/relevance of ICT systems, should be advocated, especially for systems that are necessary for the security of supply of the population or financial stability. The tests should primarily focus on critical ICT systems and their operators (e.g. financial institutions providing services for others, central ICT service providers). The criteria listed in paragraph 3 are therefore in principle comprehensible.

A repetition of TLPT at an interval of approximately 3-years in accordance with paragraph 1 represents a realistic period of time to implement measures based on the test results and to test the effectiveness of these measures.

Regarding paragraph 2: The tests should take into account the impact on the security of the company and the potential for disruption. Tests on live production systems are critical with regard to potential negative effects on production operations and may pose a direct threat to the banking business or create liability risks. Therefore, the final test design should always be determined by the tested company itself, as it is liable.

If testing of the relevant ICT services requires the participation of the relevant providers, the responsibility for this should not lie with the financial institutions. Since the actual scope of testing must be validated by the supervisory authorities, there is a risk with regards to the lack of proportionality, that banks could be made agents of the supervisory authority, even in cases where the ICT service is not critical for the provision of the process to be tested or where testing could have an impact on a large number of customers (e.g. in the public cloud, IaaS / Saas).

We do not consider a central collection of detailed documentation of vulnerabilities as well as any action plans at the supervisory authorities or third parties to be appropriate, as this increases the risk that unauthorised persons could use them (risk concentration).

Comments: Digital Finance Package of the European Commission – legislative proposal: „proposal for a regulation on digital operational resilience for the financial sector of 24.September 2020

Regarding Article 24 "Requirements for testers":

Indirect risk concentration with red teaming service providers should be avoided. Therefore, the use of a company's own Red Team resources should also be supported. This would help to solve concentration problems of test experts and also reduce risk exposure from external testing.

## Chapter V Managing of ICT Third-Party Risk

### Section I Key Principles

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 and should allow centralised operational monitoring of ICT services.

We support a proportionate approach to the management of ICT services provided by third parties as set out in Article 25, paragraph 2. The further requirements should take this principle into account. In particular, the requirements should distinguish whether or not the ICT supports critical / essential functions.

Examples:

- Article 25, paragraph 4: The required reporting to supervisory authorities on arrangements with ICT services is a new notification procedure. This should be implemented appropriately in order to avoid disproportionate efforts.
- Articles 25(5) and 26: No extensive evaluation should be required for the purchase of one-off, minor or clearly non-critical services.
- Article 25, paragraph 7: Contracts which are not based on critical ICT services should not necessarily require contractual arrangements of inspection and audit.
- Article 25, paragraph 8: 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 our understanding, this means that the institutions must ensure that they can terminate the contractual relationship without negative consequences in given cases. In principle, minimum periods should be set in consultation with the institutions concerned in order to terminate the contract.
- In the other cases mentioned above, it should also be taken into account how significant the risk is and whether the outsourcing institution may have implemented mitigating measures that address the risk of, for example, an administrative offence on the part of the ICT service provider.
- Article 27: Requirements for contractual clauses should be graded according to its risk level. The submitted requirements should only be fully applied to critical IT services.

On Article 26 ICT concentration risk:

A multi-vendor strategy 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. This problem is exacerbated by the fact that many of the services that are sourced externally are strongly tailored to the individual needs of the financial institution. Furthermore, the integration of the service provider into the outsourcing institution/group of institutions should be considered.

Irrespective of whether ICT services are purchased internally or externally, the requirement to set up a multi-vendor strategy at the level of the legal entity in particular increases the complexity in groups and reduces the added value of central outsourcing functions in groups of institutions.

Comments: Digital Finance Package of the European Commission – legislative proposal: „proposal for a regulation on digital operational resilience for the financial sector of 24.September 2020

A stronger focus on standardisation of interfaces between service providers to facilitate switching if and where it is necessary and useful would be much more targeted. Under no circumstances should the obligation be created for financial institutions to have to commit several providers in parallel for each service.

A correspondingly postulated multi-vendor strategy in certain core areas of IT would entail other significantly higher risks, depending on its design. In addition, the complexity of today's banking processes also leads to such a high level of IT complexity that only a few IT service providers are able to efficiently manage at any time and in a scaled manner for all dimensions of the institution. Due to low and qualitatively limited supply alternatives, it would not be possible to solve the concentration problem, but new concentration risks would arise. Overall, the overall risk portfolio would increase significantly.

In Germany, banks and savings banks organised in financial groups have outsourced the development and operation of IT to a large extent to central IT service providers of the respective financial group, which are controlled by the banks/savings banks. These are not "classic" third-party service providers, but rather there is a functioning and resilient division of labour in digitalization. These service providers are directly or indirectly owned by the banks and savings banks, so that the banks can assert their requirements beyond standard contractual forms. Even if the outsourcing of relevant areas of IT to a service provider entails a concentration, this outsourcing to a full-service provider always brings advantages such as an increase in the degree of standardisation, technical professionalism and the associated reduction of risk. The implementation of the legislative proposal must not endanger the structures of the savings banks and cooperative financial group, as this would have significant negative consequences for national financial market stability.

## Section II Oversight Framework of Critical ICT Third-Party Service Providers

The legislative proposal foresees a principal supervisory authority for each critical third-party ICT service provider. This is a completely new approach to the supervision of IT service providers. From the perspective of the financial institutions, 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. Overall, this must be combined with facilitations in the monitoring and provision of evidence of supervisory compliance of these ICT service providers by the financial institutions and the use of these service providers should not be made more difficult by requirements that are too limited. We therefore see a need to closely examine the proposed requirements in this chapter, but also in the chapter on ICT third-party service provider risk management in general, with a view to their necessity and targeting.

As a criterion for supervision by a European supervisory authority, a minimum condition should be that the ICT service provider operates in several Member States for financial institutions in accordance with criteria set out in Article 28(2). For significant ICT service providers operating predominantly at national level, an examination by national supervisory authorities should continue to be carried out, as they have a thorough knowledge of national circumstances.

The following aspect of the Oversight Framework poses significant risks for financial institutions:

Regarding Article 37, paragraph 3: Requests by supervisory authorities to temporarily suspend, in whole or in part, or terminate, in whole or in part, contracts between financial institutions and ICT service providers require close prior consultation with the financial institutions concerned. Priority should be given to considering whether security and risk reduction measures can be installed by the financial institutions concerned to address the risks involved. In addition, sufficient lead time is necessary for the institutions concerned.