Comments

by the Association of German Banks
“Ten points for modern third-party risk management”

11 June 2025

Lobby Register No R001458
EU Transparency Register No 0764199368-97

Diana Campar
Associate Director
Telephone: +49 30 1663-1546
diana.campar@bdb.de

Bundesverband deutscher Banken e.V.
(Association of German Banks)
Burgstraße 28 10178 Berlin | Germany
Telephone: +49 30 1663-0
www.bankenverband.de

USt.-IdNr. DE201591882

Ten points for modern third-party risk management

Increasing digitalisation and the use of added value chains in the financial sector has led to the need for a fundamental rethink of regulatory framework conditions for the management of third-party risk. Against the background of the new European Digital Operational Resilience Act (DORA), which has been in force since 17 January 2025, and the upcoming revision of the European Banking Authority's guidelines on outsourcing arrangements, the Association of German Banks supports a consistent, internationally compatible and future-oriented rulebook.

From outsourcing arrangements to third-party risk: paradigm shift required

The current regulation on outsourcing arrangements was introduced before the digital transformation of the banking industry began. Much has happened since then: Banks today are integrated into a diverse network of different third-party relationships – from the traditional service providers to cloud providers and global technology partners. The decisive factor is no longer the legal pigeonhole into which a relationship falls, but the risk that may arise from the relationship.

A future-proof regulatory approach should therefore be fully risk-based, results-orientated and not geared to any one specific technology. Assigning third parties to categories such as "Outsourcing arrangements", "ICT services" or "other external procurement" should be scrapped in future. Instead, a standardised model is required, which determines the level of risk of an activity or function solely from the importance of the institution-specific processes – irrespective of past terminology.

Harmonisation with DORA: no additional requirements

DORA sets a new European standard for dealing with ICT-related third parties. The EBA Guidelines on outsourcing arrangements, which are to be revised shortly, should be closely geared to this and not formulate any additional requirements. The principle of prioritising the application of DORA to ICT-related services must be maintained. The EBA guidelines should only apply to non-ICT-related services but should not create additional burdens.

There must be no regulatory duplication, particularly with regard to minimum contractual content, register management, due diligence and exit strategies. A consistent framework is not only a question of efficiency, but also of legal certainty and practical implementability.
A uniform approach by the European supervisory authorities is also crucial for genuine harmonisation. Despite extensive harmonisation, national specificities in supervisory practice can

lead to considerable additional burdens – especially for cross-border institutions. Fragmentation unnecessarily ties up resources that should be used for the effective management of real operational risks. Regulations should therefore not only be formally harmonised, but also uniformly interpreted and implemented in practice – in line with the EU's agenda on competitiveness and its declared political aim of simplifying regulatory requirements and making them more practicable.

Proportionality: the key to practicable regulation

Any future EBA requirements must not burden institutions with excessive complexity – small and very small institutions in particular need sufficient room for manoeuvre when it comes to implementation. A practical, proportional design is crucial to realistically take into account the different structures and resources. Instead of detailed individual requirements, principle-based regulation should take centre stage. This is the only way to harmonise flexibility, implementability and an appropriate level of supervision – without overburdening the institutions.

Outsourcing requirements must be adapted to the directly applicable and overriding DORA rules, which stipulate that size, risk structure and complexity must be taken into account during implementation, and further concretised in specific regulations.

A graduated, risk-oriented implementation model with simplifications for smaller institutions can be ensured through standardised contract components, reduced auditing requirements and the waiver of complex tests. Proportionality must be bindingly and systematically documented, accompanied by governance processes and be verifiable. Clear thresholds and standardised procedures in line with the protective objectives of supervision are therefore required for smaller institutions.

Uniform definition of critical functions: create clarity and consistency

Determining whether a third-party relationship supports a critical or essential function is a key component of a proportionate and risk-based approach to risk management. However, the definitions in the various rulebooks differ. These deviations lead to uncertainty, unnecessary complexity and inconsistency in practice.

We are therefore calling for a harmonisation of the criticality provision – both in principle and in terms of its operational effects (e.g. register management, contract content, control measures). Determining the criticality should always be process-oriented and not be extended with the addition of downstream risk analyses. The outsourcing of activities and processes that are not considered critical cannot be material per se. The purpose of the risk survey associated with

outsourcing arrangements is to ensure risk-adequate control and monitoring. It must therefore be differentiated from the process of determining criticality.

Think globally, act practically: avoiding regulatory fragmentation

For internationally active institutions, the different national and regional requirements entail a considerable amount of implementation effort. It takes a great deal of manual effort to adapt global processes and central IT systems so they comply with special national regulations – this undermines the efficiency and effectiveness of risk management.

Harmonisation must not end at the borders of the EU, which is why a standardised European approach should also take into account compatibility with international rules and standards. EU provisions should be developed with global interoperability in mind and be proportionate enough to support the competitiveness and operational resilience of businesses trading across borders.

Intra-group service providers: risk orientation instead of equal treatment

Special simplifications are required for intra-group third party relationships. A service company within a group can be managed differently than an external service provider. A sense of proportion is required here – not a complete relinquishment of control, but a differentiation in terms of risk.

Service relationships within a legal entity – e.g. between a headquarters and foreign units – should also not be categorised as a third-party relationship, as they do not represent an external provision of services in structural terms.

Subcontractors and further outsourcing arrangements: ensure proportionality

When it comes to subcontracting, DORA goes into great depth – often too much depth. Transferring these requirements to non-ICT relationships does not therefore help achieve the intended objective. A level of transparency and control geared to risk is required, and not a general principle of mistrust. Rather, the expectations of regulators and supervisors should be based on a practical and risk-based approach focussing on ‘important’ or ‘material’ subcontractors.

The materiality of subcontracting should be determined solely according to the importance of the supported function and should focus in particular on those subcontractors that play a material

role in supporting a critical or important function, the disruption of which could materially affect the provision of the service.

Focus on practicality: dealing with specialist service providers

Regulatory requirements must be designed to function even when a business cooperates with specialised niche service providers. As a general rule, the classic regulatory framework does not apply to such service providers. This poses structural limits for many banks, in particular if requirements for contractual and reporting obligations are, in practice, very difficult to fulfil. IT services for bank-owned infrastructure also suffers from the large amount of room for interpretation; there is a need for regulatory clarity. The supervisory framework conditions must take this reality into account and facilitate practical solutions, particularly for small and mid-sized banks.

Not everything is relevant: we need clear distinctions and a whitelist

Effective third-party risk management requires a clear scope of application, including information on where it does not apply. This includes, for example, office material suppliers, simple facility services or businesses already subject to supervision. Regulated services provided by financial entities should not be covered by the regulations, as including them leads to inexpedient duplicate regulations.

A clear negative list (whitelist) must be part of the regulations. Exceptions such as cooperations, joint ventures or sponsoring agreements must be treated separately – in these instances, there is no direct service or data relationship.

One register, one system: harmonise and streamline implementation

Requirements for the register and reporting must not lead to duplicate administrative work. The register structure pursuant to DORA-ITS should also be adopted for non-ICT third parties. Simultaneously, irrelevant fields should be omitted (e.g. cloud models or decision-making bodies). Registration must be centralised and harmonised, both for institutions and for supervisors. This includes ensuring a harmonised implementation process for the deadline, submission data and its validation. If national implementations of the register differ, the result will be significant operative issues across the entire sector, not to mention challenges in complying with submission deadlines.
Information and contractual requirements must be proportional to the risk, for example by grading the requirements based on the service’s degree of risk in order to avoid an unnecessary and unjustified use of resources.

Conclusion: the future is third-party risk, not outsourcing

The digital transformation will require a paradigm shift away from the outdated notion that outsourcing is an exceptional case and towards a holistic third-party risk model. Revision of the EBA guidelines is a chance to ensure that this transformation is supported by regulations. Consistency, proportionality and international compatibility must be the guiding forces behind the transition.

It’s the only way to truly effectively manage risks while simultaneously promoting innovation and guaranteeing that the European financial sector can remain competitive on the global stage.