Modernizing Europe's regulatory framework for outsourcing

Digital transformation has become a key topic across financial institutions' board rooms. Yet the regulatory framework for the implementation of technological innovations still lags behind.

The modernization of IT infrastructure is a crucial issue for many banks and financial institutions. However, the regulatory framework often fails to keep pace with technical developments and makes it unnecessarily difficult for banks to use new technologies. This has now also been recognized by supervisory authorities.

IT modernization as a decisive competitive factor

The IT infrastructure within established banks is often outdated, overly complex and in desperate need of modernization. Some banks still work with software solutions that are decades old. Financial institutions have grown and evolved through mergers and acquisitions, but often without a full IT integration or upgrade. The result is a complex infrastructure with a high proportion of manual, error-prone and slow processes in the middle and back office. The associated costs increase the pressure to modernize in a time of low returns.

The emergence of new challenger banks with lean business models, newly built IT infrastructures and fully digitalized value chains have added to this pressure, while new technological developments such as Big Data, the use of artificial intelligence, cloud solutions and distributed ledger technology (DLT) are forcing banks to modernize their IT structures. Many of the new IT solutions are now offered only in the cloud or allow the use of all functionalities only in the cloud. Distributed ledger solutions also require a modern IT infrastructure and are often combined with cloud-based solutions. A cooperation with competitors and fintechs would hardly be conceivable today without modern API-based interfaces.

> **The regulatory framework must evolve quickly to catch up: A reform of outsourcing rules is on the horizon in 2018**

IT infrastructure is not only a major cost driver, but is also a decisive factor in determining the industry's future winners and losers. Those financial institutions that succeed in quickly establishing an efficient and modern IT infrastructure and in digitalizing and continuously optimizing the value chain will be able to survive in competition.

Regulatory pressure continues

Against this backdrop, it is not surprising that supervisory authorities have started to look at the modernization of IT as one of the most important regulatory topics, not only from the point of view of risk management and IT security, but because stricter regulation increasingly requires banks to call up and link a large number of different data points at the push of a button. Finally, regulatory pressure stems from concerns about weak earnings in the banking sector and the potential disruption of traditional business models by fintechs and alternative players.

Focus on outsourcing rules

As a result, the degree and the complexity of outsourcing IT and business processes are continuously increasing in the financial industry, while the competitive landscape of service providers is also changing. Until just a few years ago, IT outsourcing solutions were tailor-made for the needs of the individual financial institution, purchased mainly from national service providers and service providers specializing in the financial sector. Now, multi-client service providers are increasingly dominating the market, promising growth in efficiency and cost reduction through standardization and the use of economies of scale. Specifically, the tech giants offer cloud-based solutions on a global basis. The importance of outsourcing regulations has also grown because many of the new IT-supported solutions are increasingly purchased as services and therefore can fall under the regulatory outsourcing rules.

Outsourcing rules: A perpetual "construction site"

Over the past 25 years, an ever-more differentiated set of rules for outsourcing in the financial sector has emerged. In Germany, the rules for credit institutions and financial services institutions are traditionally laid down by the German Federal Financial Supervisory

Authority (BaFin) in section AT 9 of the Minimum Requirements on Risk Management (MaRisk). This includes the identification and ongoing monitoring of outsourcing relationships by the risk management and internal audit departments of financial institutions. In the case of material outsourcing, the outsourcing contract has to specify in particular the rights to information and the audit rights of the internal and external auditors of the financial institutions and of the supervisory authorities. Another focus is to ensure compliance with data protection regulations and other security requirements. The supervisor also requires contractual regulation of the possibilities and conditions of sub-outsourcing and compliance of financial institutions with regulation also in case of sub-outsourcing.

In October 2017, BaFin published its latest amendment to the MaRisk, which tightened regulations on outsourcing management, adding the requirement of central outsourcing management and appointing outsourcing officers. A month later, it published its Supervisory Requirements for IT in Financial Institutions (BAIT), which further specify the rules and regulations for IT risk management, including outsourcing and other external procurement of IT services.

These provisions are principle-based and technology-neutral. For example, BaFin most recently confirmed in the BAIT that the provisions of AT 9 of MaRisk should apply without restrictions to the procurement of cloud solutions. However, neither the MaRisk amendment nor the BAIT go far enough in bringing the IT outsourcing regime up to date.

European patchwork

The outsourcing rules are poorly developed at the European level. For example, the European Union's Capital Requirements Directive (CRD IV) mentions the issue of outsourcing only in passing as part of appropriate risk management. Otherwise, the European supervisory framework for outsourcing by banks continues to be determined by the guidelines of the Committee of European Banking Supervisors for Outsourcing (CEBS) developed 12 years ago. These guidelines lay out some basic principles for a uniform supervisory framework for outsourcing. However, a full harmonization of the outsourcing rules and the practice of supervisory authorities has not been achieved. To make matters worse, a slew of other EU directives, from AIFMD, MiFID2 and EMIR to PSD2, have implemented sector-specific outsourcing rules that are also relevant for banks.

> **A patchwork of European outsourcing rules makes the group-wide sourcing of IT solutions difficult for multinational financial institutions**

The result is a European patchwork of outsourcing rules and administrative practices that makes the group-wide sourcing of IT solutions difficult for financial institutions with international operations. Although national outsourcing rules are mostly based on common basic principles and building blocks, the regulations and practice of national supervisory authorities differ considerably in detail. For example, in some countries and sectors, significant outsourcing must be notified or even approved in advance, while in other countries and sectors, periodic collective reporting is sufficient. The rules and administrative practice regarding chain outsourcing, the agreement of audit and instruction rights and the detailing of safety requirements or business continuity management also differ quite considerably. The European Central Bank's (ECB) unified supervision of the largest credit institutions in the Eurozone has done little to change this. Since many of the national regulations have been enacted at the legislative level, they do not fall within the purview of a unifying practice adopted by the ECB.

Supervisory authorities react

The European authorities have now recognized the urgent need for action. In December 2017, the European Banking Authority (EBA) launched its final recommendations for the use of cloud service providers by financial institutions. The EBA is also looking to implement a new version of the outsourcing guidelines that are intended to replace the CEBS guidelines. The ECB has recently announced that it will issue its first uniform guidelines for outsourcing by financial institutions it supervises later in 2018 and will soon launch a consultation on this subject. In addition, ECB plans to publish later this year specific guidelines for IT risk management.

ECB is due to issue its first uniform guidelines for outsourcing by major banks later this year.

At the national level, regulators and supervisors also continue to be active. In April 2018, BaFin clarified its administrative practice on rights to information, audit and control rights with respect to cloud solutions. Shortly thereafter, BaFin Chief Executive Director Raimund Röseler announced the prospect of a further revision of the outsourcing rules, particularly with regard to cloud solutions.

Technology openness instead of technology neutrality

The benchmark for the upcoming revision of outsourcing rules must be whether it enables banks to make full use of new technologies such as cloud solutions and distributed ledger technologies and to integrate these new technologies into their business models while ensuring the necessary level of risk management, security and regulatory compliance.

However, the existing regulatory framework is still strongly influenced by the model of traditional bilateral outsourcing relationships, where financial institutions purchase a tailor-made solution from a service provider and negotiate the related contract documentation with them.

This model no longer reflects the procurement processes of many of today's outsourcing services. For example, today's public cloud platforms are necessarily standardized to the highest degree so an individual financial institution has little or no influence on the global offering of the cloud service provider or the contractual structure. This results in a paradigm shift for the bank's risk

> **A rapid IT modernization and digitalization of the entire business model is becoming a matter of survival for many financial institutions**

management, as the bank's concrete use case and the associated internal risk management processes will have to be adapted to the regulatory and security requirements and the provider's standardized offer, rather than the provider adapting to the bank's individual expectations.

For the regulatory framework for outsourcing activities, financial institutions will need more flexibility so they are not hindered in the use of new technologies. A first step in this direction would be a clarification by the supervisory authorities that the audit rights of the financial institutions may also be exercised based on group audits. For example, in the case of mass procurement of standardized cloud solutions, it is neither necessary nor appropriate for each institution to audit the IT service provider individually. The EBA recommendations now explicitly provide for the possibility of group or pooled audits with other customers of the cloud providers they use. BaFin also confirms this possibility in its most recent statements, but without waiving the need for an individual right to audit.

However, the need for adaptation does not stop at audit rights. Instruction rights, which under MaRisk have to be agreed by banks with service providers "to the extent necessary", cannot be enforced against cloud providers offering their services to thousands of other companies in a standardized manner, nor do such rights make sense overall.

Against the background of global service providers with a vast number of third-party actors and multi-stage outsourcing chains, the current requirements for sub-outsourcing of services also seem excessive and unrealistic. Neither the necessity "to agree on consent requirements to the extent possible" nor the general passing on of supervisory obligations to the subcontractor appear practicable or—from the point of view of risk management—expedient and proportionate. It is not surprising then that BaFin's Röseler expressed doubts about whether "our existing rules are still really useful in practical life".

No widespread adoption of new technology without a uniform regulatory framework

For many financial institutions, a rapid IT modernization and the digitalization of the business model and of the entire value chain is becoming a matter of survival. Regulators and supervisory authorities should ensure that the regulatory framework does not hamper the use of new technologies, such as cloud solutions. Many of the new technologies help financial institutions not only to reduce costs, but are also necessary for the digitalization of their business model and also offer advantages from risk management and IT security perspectives. Widespread adoption of new technologies can only be achieved through a European regulatory framework that is technology-friendly, uniform and legally certain. In the meantime, there's hope that EBA, ECB and BaFin will take this sufficiently into account when revising their outsourcing rules.

Dr. Andreas Wieland
Partner, Frankfurt

T +49 69 29994 1337
E andreas.wieland@whitecase.com

Dr. Kirsten Donner
Associate, Frankfurt

T +49 69 29994 1655
E kirsten.donner@whitecase.com

whitecase.com

LON0618028_05