Outsourcing: An Introduction for IT Service Providers with Additional Thoughts for Financial Institutions

22.08.2024

Key takeaways

- **The outsourcing of operational functions to external IT service providers offers financial institutions economic advantages, but it also entails significant risks that must be mitigated by the involved parties.**
- **New technologies are often complex and therefore more susceptible to cyber-attacks or technical disruptions. Additional risks may also arise from subcontractors. While the realization of those risks can impact the entire value chain, these risks and their dependencies are often difficult to assess and control.**
- **Effective internal governance, sound IT knowledge, and a thorough understanding of regulatory requirements are crucial to minimizing the risks associated with outsourcing. All of these considerations must be incorporated into when drafting and negotiating the service contracts.**

Introduction

Since 1960, outsourcing - the delegation of business functions to third parties - has been a significant tool of efficient corporate management. Outsourcing allows companies to focus on their strengths and core competencies while transferring "support functions" to external service providers. Companies in the financial sector are no exception to this trend, as they increasingly outsource services to specialized providers.

For example, an asset manager can focus on the investment process while outsourcing fund administration, securities custody, or distribution to third parties. This allows for a lean organization and less capital commitment, facilitating the entry of new market participants. Another example is a life insurance company outsourcing its IT infrastructure to external IT service providers. This enables the life insurer to concentrate its internal resources on

developing new insurance products and risk assessment, while the external providers ensure efficient operations.

The growing importance of information technology (looking at topics like digitalization or cloud computing) further shows this trend. Outsourcing enables companies in the financial sector to remain technologically up to date without having to make significant IT investments themselves. However, it also makes the financial market more vulnerable to risks, particularly to risks from cyber-attacks and data breaches.

In this legal update, we discuss the legal framework and challenges associated with outsourcing activities in the financial sector. We particularly focus on the risks and opportunities related to outsourcing IT services. We provide an overview of the regulatory principles, requirements, and best practices that companies together with their IT service providers need to consider implementing their strategies.

Outsourcing in the financial sector

Principles of Regulation in Switzerland

In 1999, the Swiss Banking Commission (EBK), a predecessor of the Swiss Financial Market Supervisory Authority (FINMA), issued its first circular on outsourcing for banks (EBK Circular 99/2). FINMA subsequently restated this circular (FINMA Circular 2008/7, later replaced by Circular 2018/3) in 2009.

FINMA supervises financial institutions through a dual approach that relies on both legal provisions and so-called "circulars". This dual approach is outlined in Article 7(1) of the Financial Market Supervision Act (FINMAG). Statutory acts, like the Banking Act, form the basis for FINMA's supervisory duties. In addition, FINMA issues circulars to provide detailed guidelines and clarifications on regulatory requirements. Circulars serve to offer interpretative guidance, establish detailed rules, and promote consistency in enforcement. Although circulars are not formal laws, they have a significant impact on how financial institutions implement their legal obligations.

In addition to the outsourcing circular, FINMA has since addressed other aspects like operational risks in general or cyber incidents in other circulars and supervisory notices, that are periodically updated. Supervisory notices are specific communications issued by FINMA to address particular or urgent regulatory issues and provide additional clarifications.

In FINMA Circular 2018/3, outsourcing is defined as the situation where a company engages a service provider to independently and continuously perform a function that is essential to the company’s business operations either in whole or in part. Essential functions are those that may significantly impact a company's compliance with financial market legislation. The table below provides an overview of how FINMA, in its administrative practice, qualified certain typical outsourcing arrangements:

Outsourcing confirmed	Outsourcing denied
Complete delegation of securities operation / payment processing to a single service provider	Participation in securities settlement systems or payment systems
	Correspondent banking systems
	Physical cash deliveries and transportation
	ATM supply
Data storage / Operation and maintenance of databases / Operation of IT systems	Software development / software licensing / software maintenance
Compliance functions / internal money laundering unit	
	Legal and tax advice

Source: Appendix from FINMA Circular (Cs) 2008/7 (repealed)

The table only reflects the general concept. Of course, the specific circumstances of each case must always be examined. In general, delegating functions that involve the direct communication with many customers qualify as outsourcing. On the other hand, subordinate support services for the investment process, such as creating and presenting strategic asset allocations and model portfolios without involving customer data, may still qualify as non-essential and remain out of scope for the outsourcing circular. Whether software development or software maintenance should still be considered outsourcing seems debatable today when looking at newer phenomena such as Software-as-a-Service solutions and cloud computing.

In essence, FINMA circulars and notices are based on the broadly defined requirements for adequate organization in the various financial market laws that apply to banks, financial institutions, and insurance companies.Specific Regulations for Financial Institutions

Specific Regulations for Financial Institutions

For financial institutions regulated under the Financial Institutions Act (FinIA) since 1 January 2020, i.e., asset managers and trustees, managers of collective assets, investment firms (securities dealers), and fund management companies, there are specific requirements for outsourcing at the statutory level. However, neither the law nor its implementing ordinance (FinIO) uses the terms "outsourcing" or "delegation". Instead, the law refers to the "transfer of tasks" (Article 14 FinIA, Article 15 FinIO). A transfer of tasks, according to Article 14(1) FinIA, occurs when a financial institution engages a service provider to independently and continuously perform an essential task, either in whole or in part, and this results in a change to the facts underlying the financial institution's license. It would be more practical for all supervised institutions, including banks, insurers, and financial institutions, to refer to significant outsourcing, which is subject to additional regulatory provisions while other outsourcing arrangements could be governed by general contractual rules. (This is like the distinction made in German law, see Article 25b of the Banking Act (KWG)).

The law and the ordinance specify which tasks are considered to be essential for each type of financial institution, and thus fall under the provisions for task transfers:

Asset managers and trustees	Managers of collective assets	Fund management companies	Investment firms
▪ Portfolio management ▪ Investment advice ▪ Portfolio analysis ▪ Offering of financial instruments.	▪ Portfolio management ▪ Risk management	▪ Fund business ▪ Custody ▪ Administration	▪ Securities trading ▪ Issue of derivatives

Since 2020, the scope of FINMA Circular 2018/3 on outsourcing, originally issued only for banks and insurers, has explicitly included asset managers, fund management companies, and investment firms. For insurance companies, notification and prior approval from FINMA are required (Article 4(2)(j) of the Insurance Supervision Act). Depending on the specific circumstances, they may need to either notify FINMA of the planned outsourcing or obtain prior approval (Articles 8 and 10 FINIG).

Contrary to the wording of Article 14(1) FINIG, all outsourced activities, including those considered "non-essential", must be reported to FINMA when applying for authorization. FINMA assesses on a case-by-case basis whether an outsourcing is significant or not. For instance, according to current FINMA practice, outsourcing of risk management and compliance is considered significant for asset managers and trustees, as are activities such as managing trust assets, IT services, or trust accounting. Generally, FINMA tends to view outsourced activities as significant.

Therefore, it is advisable to apply FINMA Circular 2018/3 on outsourcing analogously to asset managers and trustees, even though they are not formally included in the circular. Particularly, asset managers and trustees must establish fundamental principles for delegations, including the conditions under which delegation is permissible, how instructions are given within the delegation. Delegation agreements must always be in writing. Contracts must grant FINMA, supervisory organizations, and auditors the right to full, unrestricted, and ongoing access and review of the outsourced function.

New Insights from Supervisory Practice

Networking Implies Risk

Outsourcing of financial services has significantly increased in recent years. According to the FINMA Risk Monitor 2023, over 60% of supervised companies outsource critical areas, primarily IT services. Areas particularly affected include cloud computing, data processing, and cybersecurity. In some sectors of the financial industry, the supervised firms rely on a few specialized IT providers, which creates a kind of "digital monoculture". Such a centralized model can lead to severe problems: the failure of a critical service provider could have significant consequences, as technologies become increasingly complex and susceptible to cyber-attacks or technical disruptions. Particularly concerning are so-called "zero-day attacks", where attackers exploit previously unknown vulnerabilities before protective measures can be implemented. These attacks pose a considerable challenge for supervised companies, as these vulnerabilities are often difficult to identify with conventional security measures. An example is the MOVEit incident, which demonstrates how the failure of a multi-tenant service provider can cause significant disruptions to many companies simultaneously - financial institutions are no exception. MOVEit was targeted in an attack that exploited security gaps, leading to major disruptions and data losses. Another example is the recent incident with CrowdStrike. These failures can trigger a cascading effect, adversely affecting either a single financial sector or the entire financial market. Additional risks may arise from the further delegation of IT services to subcontractors, as issues with a subcontractor can impact the entire value chain. These dependencies and risks are often difficult for outsourcing companies in the financial sector to assess and control.

This general trend is further highlighted by recent developments such as "Modular Finance" or "Open Banking". The Swiss Bankers Association (SBA) defines Open Banking as a business model based on the standardized and secure exchange of data between the bank and trusted third-party providers. Third-party providers may also include other financial service providers. But, the value chain of banking and financial services, distributes it among various highly specialized providers, and, through digital tools, reconnects it into a unified client experience for customers.

	Outsourcing	Open Banking
Control over performance of services	Bank	Third party
Consent of the customer necessary?	No	Yes
Influence on value chain	Integrated	Dependent on the business strategy
Third party acts ...	...on behalf of and in the interest of the Bank	...mainly in the interest of the customer

Source: Swiss Bankers Association

Some Statistics from Germany

As previously discussed, outsourcing impacts the internal organization of a company. Typically, outsourcing activities are not reported, making it difficult for outsiders to gauge the quantitative significance of this issue, the most important entanglements that arise. For Germany, the Federal Financial Supervisory Authority (BaFin) recently illustrated the tight interconnections. Since the generalization of the reporting requirement for significant outsourcing in 2021/2022, approximately 1,900 supervised companies have reported around 20,800 new significant outsourcings. On average, this results in about 11 significant outsourcings per company. Graphical representations (network graphs) enable the authority to identify concentrations on specific service providers operating as multi-tenant providers. Outsourcing structures within individual contractual relationships can also be visualized, particularly regarding further outsourcing to subcontractors (service provider chains). Such service provider chains are – evidently – not uncommon. As previously noted, they can become problematic when disruptions at a subcontractor cascade to other parties, potentially affecting an entire group of financial institutions.

This reflects the observation that the financial sector is increasingly dependent on technology itself and technology companies for providing financial services. As recent years have made clear, this makes financial institutions vulnerable to cyber-attacks or other incidents. This is where DORA, the European Digital Operational Resilience Act (Regulation (EU) 2022/2554), comes into play, which will take effect from January 17, 2025. DORA includes provisions on ICT risk management, ICT partner management, stress tests, incident reporting, information shared between supervisory authorities, and a "light-touch" supervision for critical service providers.

Article 17 DORA requires both the financial institutions themselves and certain critical service providers to establish, maintain, and operate processes for managing ICT-related incidents to detect, address, and report such incidents. The regulation is based on the notion that incident reporting is important not only for the affected company, but it serves the entire financial market.

New Swiss Reporting Obligations for Cyber Incidents

With the FINMA Supervisory Notice 05/2020 "Reporting Obligation for Cyber Attacks According to Article 29(2) FINMAG", the obligation to report cyber-attacks to FINMA, based on the general reporting duty, was further defined. According to FINMA, the reports received since then have shown varying developments in the threat landscape, attack methods, and targets of attacks.

FINMA Supervisory Notice 03/2024 builds on these insights and emphasizes the need for a proactive approach to cyber risks, particularly through the monitoring of service providers. It has been observed that only "very few institutions proactively" contacted their key service providers after identifying serious security vulnerabilities. This gap in risk management may be due to the lack of a complete and up-to-date inventory of their service providers. Although the FINMA Circular 2018/3 – "Outsourcing" already requires financial institutions to maintain a detailed and current inventory of their service providers to have a comprehensive overview of all external service providers and their importance for the operational security and stability

of the company, this requirement is often not adequately, consistently, and/or continuously implemented. It is evident that without such an inventory, it is very difficult to determine whether critical data is stored with a service provider or if the provider is tasked with delivering a critical function.

Therefore, FINMA Supervisory Notice 03/2024 calls for enhanced measures, like the regular review of the cyber security of service providers and the conduct of scenario-based cyber risk exercises. To minimize the risk of cascading effects of cyber incidents on financial institutions and their service providers is key.

Next Steps

Today, banks and other financial service providers must excel in two areas that have little to do with the traditional finance world: In addition to strong internal governance, they must first be proficient in IT. Second, they need to be well-versed in regulatory issues to communicate constructively with regulatory authorities.

Most institutions today do not rely solely on their own IT capacities (though there are, of course, well-known exceptions). Institutions that depend on external service providers are well-advised to create a comprehensive inventory independently of whether they are required to do so like larger banks. They must clearly define what constitutes critical data and where it is stored. They must categorize their service providers appropriately and work with them to define and contractually agree on the necessary control measures to mitigate identified risks. Effective internal governance and disciplined stakeholder management for critical service providers are essential for a defense against cyber incidents and other IT risks.

IT service providers themselves are not subject to Swiss regulations. However, since institutions are required to incorporate outsourced processes into their risk management frameworks, IT service providers have a strong incentive to support their clients' risk management. Therefore, IT service providers in the financial sector must be knowledgeable about financial market regulations.

In this context, Artificial Intelligence (AI) may be not only "part of the problem" but also part of the solution. AI may help automate the monitoring and analysis of IT service provider activities to detect and respond to potential security risks early. AI systems may also assist in monitoring and ensuring compliance with performance indicators (KPIs) and service-level agreements (SLAs). Additionally, AI enables continuous adjustment of protective measures to new threats and regulatory requirements.

The interplay between financial institutions and IT service providers must be governed and documented in service contracts. These contracts should be drafted by legal professionals while technical specialists must ensure that operational details are precisely defined. The contract should include KPIs, SLAs, and security and emergency protocols.

It is important that business representatives see their requirements reflected in the executed contract and that regular reviews and adjustments are made to meet current needs and developments. This ensures that the collaboration is efficient, compliant with the law, and minimizes risks. The use of AI can play a crucial role in achieving these goals, and it further

strengthens the security architecture of financial institutions.

Authors: Markus Winkler (Counsel), Xenia Pisarewski (Associate), Armina Burkic (IT Analyst)

No legal or tax advise

This Legal Update provides a general overview of the legal situation in Switzerland and makes no claim to completeness. It does not constitute legal or tax advice. If you have questions about this Legal Update or need legal advice concerning your situation, please contact your representative at Pestalozzi Attorneys at Law Ltd. or one of the contacts mentioned in this Legal Update.

Andrea Huber

Partner
Attorney at law, LL.M.

Pestalozzi Attorneys at Law Ltd
Feldeggstrasse 4
8008 Zurich
Switzerland
T +41 44 217 92 41
andrea.huber@pestalozzilaw.com

Markus Winkler

Counsel
Attorney at law, Dr. iur.

Pestalozzi Attorneys at Law Ltd
Feldeggstrasse 4
8008 Zurich
Switzerland
T +41 44 217 92 59
markus.winkler@pestalozzilaw.com