Baker McKenzie.

Bite-size Briefings

October 2022 Ed. No. 10

A series of briefings that take a "bite-size" look at international trends in different jurisdictions, drawing on Baker McKenzie's expert financial services practitioners.

Bite-size Briefings: Outsourcing regulation — October 2022

This edition explores developments in outsourcing regulation across Germany and the EU, Hong Kong SAR, Singapore, Switzerland, the UK and the US.

Outsourcing service providers, which often sit outside the regulatory perimeter, are fast becoming an integral part of the financial infrastructure. This is because many financial institutions are becoming progressively more dependent on outsourcing due to its ability to reduce costs and, for digital services, to adopt and scale new technology more quickly, accelerating their digital transformation.

While, for example, cloud services offer advantages, such as economies of scale, flexibility, operational efficiencies and cost effectiveness, outsourcing can also present challenges in terms of data protection, banking secrecy, security issues and concentration risk. These are challenges not just for individual businesses, but also at a systematic level because large providers risk becoming a single point of failure where many institutions rely on them.

Regulators are increasingly concerned about operational resilience and continuity of service, not just for in-house systems and controls, but also in outsourced services. A further issue arises where providers, in effect, may be the dominant party such as banking-as-a-service or if they carry on licensed activities. All this is reflected in growing regulatory scrutiny of outsourcing and the issue of regulatory requirements and guidelines to regulated institutions. As we discuss below, in some jurisdictions there are proposals to grant regulators supervisory direct powers over some providers.

UK

In a move highly anticipated by the industry, the UK Treasury has confirmed that it will implement a regime whereby third-party firms designated as "critical" will be subject to direct regulatory oversight. The UK Treasury published a **policy statement** in June 2022, setting out its framework for mitigating the risks caused by financial services firms outsourcing important functions to third-party service providers; shortly after, the legislative framework was introduced to Parliament in the Financial Services and Markets Bill 2022-23.

The forthcoming regime seeks to plug the systemic risk gaps left open by the UK's current operational resilience framework when a third party provides critical functions to multiple firms in the financial services sector. Under existing requirements, firms must ensure that their contractual arrangements with third parties allow them to comply with the regulators' operational resilience framework; but these requirements do not extend to the third-party firms themselves. If several firms rely on the same third party for material services, the failure or disruption of this third party could have a systemic impact across the financial sector.

The framework will enable the UK Treasury, along with the Bank of England, the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) (the financial regulators), to directly oversee third-party service providers. Under the regime, the UK Treasury will consult with the financial regulators before designating certain third parties that provide services to firms as "critical" (CTPs); it will also be possible for the financial regulators to proactively recommend CTP designation. The UK Treasury will also need to have regard to representations made by potential CTPs as well as financial services firms. CTP designation is expected to take into account factors such as the number and type of services a third party provides to firms and the materiality of these services and will be formalized in secondary legislation.

Once a third party is designated as a CTP, the financial regulators will be empowered to make rules, gather information and take enforcement action in respect of material services that CTPs provide to firms. These powers will include the ability to set minimum resilience standards that CTPs will be directly required to meet in respect of any material services that they provide to the UK finance sector, together with additional information-gathering and investigatory powers to assess whether resilience standards were being met, the power to direct CTPs from taking (or refraining from taking) specific actions, and enforcement powers to remedy breaches.

The Bill is currently undergoing the legislative process, with Royal Assent expected in 2023. The FCA and PRA issued a **joint discussion paper** in July 2022 setting out how they intend to use the powers that they have been granted, with responses requested by 23 December 2022. Following Royal Assent and feedback from the discussion paper, the regulators will publish a consultation paper setting out the proposed rules. Once the regulatory rules are finalized, the UK Treasury will begin designating CTPs.

Although the introduction of the new framework will place significant new regulatory burdens on designated CTPs, the population of affected third-party service providers is expected to remain small, at least in the short term, as the market for these services tends to be highly concentrated. In particular, **analysis** from the Bank of England highlighted that, as of 2020, over 65% of UK firms used the same four cloud providers for cloud infrastructure services.

Third-party service providers should keep a watching brief as legislation is introduced and more information becomes available about the criteria to be used for designation to assess whether they could be caught by the new framework. Although financial institutions will not be directly affected by the new CTP framework, they will remain accountable for managing risks to their operational resilience and should begin to consider how the CTP framework should be integrated into their own operational resilience policies and processes (for example, whether contractual terms might need to be modified).

EU

The UK's CTP framework is similar to the oversight regime for critical information and communication technology (ICT) third-party service providers set out by the EU Commission in its proposed Regulation on digital operational resilience for the financial sector (widely referred to as the Digital Operational Resilience Act (**DORA**)), although the two regimes take different approaches. Under DORA, the European Supervisory Authorities (ESAs) will designate the ICT third-party service providers that are critical for financial entities, which will then become subject to oversight in relation to their resilience from the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) or the European Insurance and Occupational Pensions Authority (EIOPA) as lead overseers.

The approach to designation set out in DORA is much more granular and harmonized than that to be expected under the UK's CTP framework. At a high level, DORA requires the ESAs to consider designation criteria, including the systemic impact of the services, the systemic importance of the financial institutions relying on the services, critical or important functions provided, substitutability and number of member states involved — and the Commission is further empowered to adopt delegated acts supplementing these criteria. By contrast, the approach adopted by the UK Treasury is much more discretionary, in keeping with its general post-Brexit approach to financial services regulatory reform.

After designation, the lead overseer must assess whether the critical ICT third-party service provider has in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risks which the provider may pose to financial entities, and adopt an individual oversight plan for the provider based on this assessment. The lead overseer is also granted similar information-gathering and investigation powers as those granted to the UK financial regulators under the UK's CTP framework, as well as the powers to issue recommendations and impose financial penalties. However, whether DORA and the UK's CTP framework will significantly diverge in practice remains to be seen, with much of the detail forthcoming in technical regulatory standards from the ESAs and in detailed rule proposals from the UK financial regulators.

The Council of the EU and European Parliament reached provisional political **agreement** on DORA in May 2022. Formal adoption by both institutions will now follow, with the European Parliament expected to consider DORA in plenary in November 2022, followed by publication in the Official Journal and entry into force in late 2022 or earlier 2023. DORA will apply 24 months after entry into force.

Germany

German regulation of third-party service providers is shaped by its membership of the EU together with its domestic requirements. In addition to the forthcoming DORA framework (as explained above), key recent developments regarding cloud outsourcing in Germany concern: i) the implementation of the EBA Guidelines on outsourcing; ii) the implementation of the ESMA Guidelines on cloud outsourcing; and iii) legislation introduced in the wake of the Wirecard scandal in Germany referred to as FISG.

EBA and guidelines

Regarding the **EBA Guidelines**, instead of simply declaring them domestically applicable, the German regulator, BaFin, modified its circular "Minimum Requirements on Risk Management" (**MaRisk**) in August 2021. Section AT 9 of it simply details the German regulatory outsourcing regime for banks and financial services providers and requires close scrutiny. As a result, it is difficult to use standard checklists that were prepared to track compliance with the EBA guidelines and it is unclear whether MaRisk contains additional requirements (over and above the EBA Guidelines).

As a side note, since the regulation of investment firms has been removed from the German Banking Act, these are now regulated in the new Securities Institution Act (except for large so-called "Class 1" firms), and technically, MaRisk no longer applies to investment firms. However, since BaFin has not yet created a separate lighter-touch risk management regime for investment firms, MaRisk continues to apply to them in the interim.

In contrast, BaFin has implemented the **ESMA guidelines** on cloud outsourcing by simply declaring them applicable in a notice published in June 2021. The problem is that BaFin failed to clarify whether this makes its earlier guidance on cloud outsourcing obsolete regarding investment firms and fund managers. The BaFin guidance note on cloud outsourcing was meant to summarize the requirements for cloud outsourcing across all regulated sectors. We take the view that the ESMA guidelines have not superseded the BaFin's guidance on cloud outsourcing, since the two papers cover different aspects of cloud outsourcing.

FISG

Another interesting development concerns the tougher rules on outsourcing in the **FISG**, which entered into force on 1 July 2021. Under the FISG, all regulated firms need to notify BaFin of their intent to outsource a material activity. Before the FISG came into force, this rule applied only to insurance undertakings. Moreover, regulated companies must notify BaFin of material changes and serious incidents arising from outsourcing. Under the FISG, there is a statutory obligation on firms to maintain a register of outsourced activities.

Crucially, under the FISG (and foreshadowing forthcoming DORA requirements), BaFin can directly issue instructions to outsourcing service providers. For this purpose, non-EEA outsourcing providers must appoint an agent in Germany for service of such BaFin orders. BaFin is permitted to issue orders (i) that are suitable and required to prevent or stop breaches of regulatory rules or (ii) to prevent or remove deficiencies concerning the regulated company, which could endanger the security of client assets or impair the proper conduct of business or services. In the case of fund management companies, such an order can also be issued to prevent the fund manager from becoming a letterbox entity. These powers are rather broad fashioned and outsourcing providers should consider appropriate protections in their outsourcing agreements, e.g., for increased costs or losses resulting from compliance with such an order.

Hong Kong SAR

Ensuring ongoing operational resilience of financial institutions when using external providers has been a long standing theme for the Hong Kong financial services regulators: the Hong Kong Monetary Authority (HKMA) and the Securities and Futures Commission (SFC). Requirements aimed at ensuring ongoing integrity and resilience associated with the use of third party service providers have included, but are not limited to, the HKMA's **Outsourcing requirements**, the SFC's endorsement of the Principles on Outsourcing of Financial Services for Market Intermediaries published in 2005 by the International Organisation of Securities Commissions (IOSCO), (as subsequently been **amended** by IOSCO in 2021), and detailed Electronic Data Service Provider requirements **issued** by the SFC in 2019, supplemented by FAQs in 2020.

In October 2021, the SFC issued a **circular** to Intermediaries releasing operational resilience standards and required implementation measures to supplement the SFC's existing guidance on areas including cybersecurity, business continuity plans, internal controls and risk management. The circular also included a "**Report on Operational Resilience and Remote Working Arrangements**" and established a new Operational resilience standard on third party dependency risk management. The new standard requires intermediaries to implement measures to identify, contain and manage third party dependency risks. These include, for example, undertaking reviews at suitable intervals or whenever there are changes in key service providers and ensuring that the risk of loss (financial or otherwise) is at acceptable and appropriate levels.

On 31 May 2022, the HKMA issued a new Supervisory Policy Manual (SPM) module OR-2 on Operational Resilience and a revised version of SPM module TM-G-2 on Business Continuity Planning. The new OR-2 provides high level guidance to reflect the HKMA's expectation that all authorized institutions (AIs) will be operationally resilient. The requirements of OR-2 include addressing third-party dependency management. In order to reduce the risk associated with the use of a third party, amongst other requirements AIs are expected to ensure that the third party has equivalent operational resilience to the AI. Where this is not possible, they are expected to satisfy themselves that the third party engagement will not weaken their ability to deliver critical operations in the event of a disruption and there should be arrangements in place to satisfy themselves on a continual basis that adequate operational resilience is maintained by the third party. Further, consistent with normal BCP arrangements, an AI should have in place appropriate BCP arrangements and exit strategies which address the failure or disruption to the services provided by the third party. AIs are expected not to enter into or continue any arrangements with third parties that would weaken the operational resilience of any of their critical operations. The revised TM-G-2 aims to complement the requirements of OR-2 by enhancing existing guidance on business continuity planning. The HKMA requires all AIs to have (i) developed an operational resilience framework and determined the timeline by which it will become operationally resilient, within 1 year after the final OR-2 module was issued (i.e. by 31 May 2023); and (ii) become operationally resilient as soon as their circumstances allow and no later than 3 years after the initial 1-year planning period (i.e. by 31 May 2026).

The HKMA has further supplemented these requirements with the issue in August 2022 of its **Guidance on Cloud Computing**. The guidance aims at consolidating various existing requirements. They include requirements to address potential concentration risk, such that AIs should keep under regular review factors including: (i) the possibility of cloud portability; (ii) the availability of interoperability solutions; (iii) the feasibility of adopting a multi-cloud strategy; and (iv) whether viable exit strategies are in place to enable an orderly exit when needed, particularly under a stress scenario. The HKMA considers that AIs should also take into account and manage any potential supply chain risks that may impact the provision of services by the cloud service provider. AIs are also required to have in place appropriate contingency plans to address disruption of cloud service providers and satisfy themselves that a disruption will not impact an AI's operational resilience.

Singapore

The Monetary Authority of Singapore (MAS), Singapore's central bank and integrated financial regulator, expects all financial institutions to ensure that the third-party service providers they rely on for service delivery are subject to adequate governance, risk management and sound internal controls. MAS also requires senior management to assess the risks from third-party services and implement controls commensurate with the nature and extent of these risks. In recent years, financial institutions have reported a variety of interruptions to digital banking services and while the root

causes lay mainly with them, at least one arose from an outage in a third-party cloud service provider. Here, MAS expects firms to be able to recover systems supporting critical banking services within hours.

MAS' **Guidelines on Outsourcing** define outsourcing arrangements as those where a service provider provides a service that the financial institution may perform itself. Additionally, financial institutions must be dependent on the service on an ongoing basis, which must be integral to the provision of a financial service by the financial institution, or the service is provided to the market by the service provider in the institution's name (e.g., banking-as-a-service). The guidelines also include non-outsourcing arrangements (NOAs), which refer to third-party arrangements with service providers that fall outside the definition of outsourcing arrangements, but nevertheless are subject to adequate risk management and sound internal controls. Of relevance here, MAS has also published **Technology Risk Management Guidelines**.

Under MAS' recently revised **Business Continuity Management Guidelines** (BCM Guidelines), financial institutions should take into account third-party dependencies when engaging third parties to support the delivery of their critical business services. The revisions aim to ensure strengthened resilience against service disruptions due to IT outages, pandemic outbreaks, cyberattacks and physical threats. With regard to outsourced critical business functions, the BCM Guidelines identify the likelihood of concentration risk when several of an institution's critical business functions are outsourced to a single provider. They make recommendations to mitigate concentration risk such as separating primary and secondary sites of critical business services or infrastructure (e.g., data centers) into different zones to mitigate wide-area disruption. Senior management responsible for business continuity management (BCM) must familiarize themselves with the guidelines, which MAS expects financial institutions to meet within 12 months of issuance. It will conduct the first BCM audit within 24 months of issuance.

In August 2022, MAS published an information paper, **Operational Risk Management - Management of Third Party Arrangements**, after conducting inspections on selected entities. MAS observed that, although financial institutions generally have established frameworks and processes to manage outsourcing arrangements, some fall short of expectations in managing oversight and risk reporting of outsourcing activities, as well as due diligence and ongoing monitoring processes (e.g., due diligence is not completed on a timely basis and concentration analyses are not performed). For NOAs, some financial institutions did not have robust frameworks to manage such arrangements, or were at a nascent stage of developing controls to manage the associated risks. MAS additionally found some entities were still at an early stage of setting up a third-party governance structure, and were largely managing their NOAs in a decentralized manner through respective business units, when it would have preferred the consolidated oversight of a management committee.

New legislation

The new **Financial Services and Markets Act 2022** (FSMA), when in force, will enable MAS to adopt a financial sector-wide regulatory approach to complement its existing entity and activity based regulation. Among the key aspects are MAS' harmonized and expanded power to issue prohibition orders and its harmonized power to impose requirements on technology risk management. MAS will be able to prohibit service providers that have demonstrated by their misconduct the potential to cause harm in the financial industry. Additionally, Section 6 extends the **Guidelines on Fit and Proper Criteria** to ensure financial institutions appoint fit and proper service providers to undertake key roles, functions and activities, thus requiring financial institutions to check that their service providers' relevant employees who undertake functions are not prohibited from doing so.

The FSMA obligations on outsourcing are in line with developments to ensure that financial institutions enhance their oversight of outsourcing arrangements, such as MAS' Guidelines on Outsourcing and recent Banking Act amendments to enhance MAS' supervisory oversight of banks' outsourcing arrangements.

Switzerland

There have been two key recent developments on financial services outsourcing in Switzerland. These concern first, the implementation of a draft supervisory circular to strengthen banks' operational resilience by the Swiss Financial Market Supervisory Authority (FINMA) and second, considerations over the use of decentralized securities and IT infrastructures based on distributed ledger technology (DLT).

FINMA's efforts to strengthen banks' operational resilience will have a significant impact on IT outsourcing providers. Rules on operational resilience aim to ensure that banks have the ability to overcome significant shocks in a timely manner with minimal negative impact. This could be a pandemic, a natural disaster or even a supply chain failure or cyberattack. To do so, banks must identify critical operations whose interruption would jeopardize the continuation of the institution or its role in the financial market and thus the functioning of financial markets. In comparison to the concept of business continuity management, operational resilience has more depth, but is narrower in scope.

Supervisory circular

The draft **circular** and FINMA's explanatory notes make clear that the involvement of third parties will be essential, explicitly naming cloud providers that will be affected. Hence, outsourcing providers whose services fall within the scope of critical functions must expect additional demands from the banks' side: support in the context of scenario planning, increased controls, integration into the control processes of the outsourcing banks and exercises to test plans.

DLT services

Where financial institutions use DLT service providers, a key aspect when dealing with DLT-based customer products is data protection. To the extent that neither client-identifying data (CID) nor any other personal data is stored on a distributed ledger, there are no client confidentiality, banking secrecy or data protection obligations to be observed. Swiss bank secrecy is always linked to CID. However, indirect relationships between, for example, pseudonymized data and CID in clear form (i.e., CID in the proper sense) must be considered under bank secrecy. In particular, financial institutions must ensure that unauthorized third parties cannot combine pseudonymized data with additional information sourced from other, possibly multiple, sources and thereby identify a client. This applies in both an outsourcing scenario and where a financial institution itself processes data on the ledger.

If securities are booked on DLT, for example, by tokenizing such securities as a Swiss ledger-based security, the use of protocols such as Ethereum, tezos or other DLT applications would arguably be considered an outsourcing arrangement under the applicable financial services laws and regulations. However, a degree of uncertainty remains and the future practice of regulatory authorities and the courts will provide more light on this point. On the basis that the arrangement is similar to participating in a financial market infrastructure such as a securities settlement or payment system, one may take the view there is solid ground to argue that the use of DLT does not qualify as outsourcing within the meaning of FINMA Circular 2018/3. FINMA, however, has previously stipulated data storage, as well

as the operation and maintenance of databases and IT systems, as outsourcing which is subject to the relevant regulatory requirements of FINMA. Therefore, certain services performed with DLT applications, whether these are run directly by the financial institution or a third-party service provider, may meet the definition of "outsourcing" under Swiss financial market laws.

US

Financial institutions rely on third-party partners and vendors for a range of products and services that is both broad and business-critical. Vendors and partners provide a wide array of software, operational technical support and solutions for trading, client interfaces, data storage, as well as a range of outsourced services, such as communications capture and production, provision of so-called "alternative data" and cyber security. No "Bite-size Briefing" could contain the full listing of all of the ways that financial institutions depend on third parties to get the job done every day.

Regulated entity responsibility

For all of these products and services, regulators have always looked to the regulated entity to ensure that the purchased product or service is actually working in a compliant fashion; when trouble ensues, it is the regulated entity that is held responsible. This has been so whether or not the regulated firm actually has visibility into the product. Thus, for example, if a vendor fails to implement a firm's instructions — even written instructions — into software related to trading limits, the broker-dealer will be held responsible by the regulator when entered trades exceed limits in those written instructions, resulting in errors and potential Market Access Rule violations. This is because vendors and other third parties fall outside of limited regulatory jurisdiction. As a result, financial regulators have consistently warned the regulated, for example, in this Financial Industry Regulatory Authority (FINRA) **Regulatory Notice**, to document, implement and test policies and procedures to review all work and products provided by vendors, such as cybersecurity controls, and to actively manage vendor engagements, particularly those with access to client information.

This thread was also picked up in the 2022 **Report** on FINRA's Examination and Risk Monitoring Program. In the report, FINRA raises many of the same concerns as those cited in the regulatory notice, including about cybersecurity and vendor controls generally. Further to the example noted above, FINRA also asks whether firms use third-party tools or vendors to comply with Market Access Rule obligations, and notes examination findings that firms may rely too heavily on vendors without sufficient testing or controls. FINRA's report also specifically identified considerations for firms relating to vendor-assisted books and records retention, like cloud service providers, and queries how confidential material is stored, and whether it is retained in conformity with recordkeeping rules, including electronic storage media standards.

SEC rules for service providers

Finally, on 26 October 2022, on the initiative of the Division of Investment Management of the US Securities and Exchange Commission (SEC), the SEC proposed new **rules** relating to the role of certain third-party service providers in the asset management industry. The proposed rules aim to mitigate the risk of investor harm, for example, by introducing requirements on pre-engagement due diligence and ongoing monitoring. Earlier this year, on 15 June 2022, the SEC issued a **notice** seeking public comment regarding whether certain information providers, such as index providers, model portfolio providers and pricing services are, in some circumstances, acting as investment advisers under the Investment Advisers Act, such that they should be required to register with the agency.

Contacts

Germany

Manuel Lorenz

Partner
manuel.lorenz
@bakermckenzie.com

Subatra Thiruchittampalam

Associate
subatra.thiruchittampalam
@bakermckenzie.com

Hong Kong

Karen Man

Partner
karen.man
@bakermckenzie.com

Aaron Dauber

Registered Foreign Lawyer / Knowledge Lawyer
aaron.dauber
@bakermckenzie.com

Singapore

Stephanie Magnus

Partner
stephanie.magnus
@bakermckenzie.com

Sek Cheong Yong

Knowledge Lawyer
sek.cheong.yong
@bakermckenzie.com

Switzerland

Ansgar Schott
Partner
ansgar.schott
@bakermckenzie.com

Yves Mauchle
Associate
yves.mauchle
@bakermckenzie.com

United Kingdom

Mark Simpson
Partner
mark.simpson
@bakermckenzie.com

Kimberly Everitt
Knowledge Lawyer
kimberly.everitt
@bakermckenzie.com

United States

Amy Greer
Partner
amy.greer
@bakermckenzie.com

Jennifer Klass
Partner
jennifer.klass
@bakermckenzie.com

Global Editor

Richard Powell
Lead Knowledge Lawyer
richard.powell
@bakermckenzie.com

One Global Financial Services Regulatory Team

The financial services industry is undergoing sweeping changes driven by regulatory developments, rapidly advancing technology and continued consolidation in the sector. The far-reaching impact of financial reforms, intricacies in their implementation, and conflicting regulations in different jurisdictions can expose businesses to unforeseen risk.

Our global team provides financial institutions guidance on navigating through regulatory complexities in both established and emerging markets. Our lawyers have long-standing relationships with financial services regulators, and are experienced in helping financial institutions deliver financial services efficiently and cost-effectively in a compliant manner.

From set-up and structuring, new business and product offerings, operational support as well as representation in non-contentious and contentious matters, we apply our industry knowledge and regulatory expertise to deliver result-oriented and compliant solutions for all types of financial institutions including banks, insurance companies, payments companies, securities firms and asset managers.

bakermckenzie.com