Technology outsourcing in the Saudi financial services sector: The SAMA Outsourcing Rules

Nick O'Connell - Partner, Head of Digital & Data - Saudi Arabia - Digital & Data - Riyadh

There have been significant changes in technology and regulation since 2008, when the Saudi Arabian Monetary Authority (SAMA) issued Circular No. 424 B.C.S / 34720 – the SAMA Rules of Outsourcing Processes. In this article, we summarise key aspects of the "Outsourcing Rules" with a focus on the outsourcing of information technology services.

Outsourcing is a business practice in which a business engages external service providers to perform certain business functions, instead of having those functions performed by its own personnel. The increasing complexity of the outsourcing arrangements adopted by banks, and the potential harm to consumers from offshoring arrangements out of reach of regulators, led to a 2005 report by the Basel Committee on Banking Supervision. The report contained recommendations about tightening the way in which banks outsourced their activities. SAMA subsequently issued the Outsourcing Rules in 2008.

The stated objective of the Outsourcing Rules is to provide guidance to banks on how to arrange outsourcing, while remaining compliant with the obligations under their banking licences. The Outsourcing Rules apply to branches of foreign banks in the Kingdom, as well as to domestic banks licensed under the Banking Control Law issued under Royal Decree No. M/5 dated 22/2/1386H (12 June 1966).

Engaging third party service providers can enable banks to reduce costs and obtain other efficiencies, but it may also expose banks to a variety of risks. These can include operational and reputational risks, such as when service providers fail in their performance, when security or confidentiality breaches result, or where the service providers' actions otherwise result in banks failing to comply with statutory or regulatory obligations. Additionally, the whole banking sector could be at risk if a common service provider to a number of banks fails in its performance of the services entrusted to it.

Outsourcing basic work and non-basic work

The Outsourcing Rules split those functions and tasks that can be outsourced into two main categories – ‘basic works’ and ‘non-basic works’. There are different considerations for outsourcing each of these categories of works, and there is a general prohibition (with some exceptions) on the outsourcing of works relating to customer data processing.

Basic Works

Basic works refer broadly to the core tasks and responsibilities that banks have towards their customers. The operation of a bank’s information technology system is a prime example of basic works. Other examples include all customer-facing tasks (e.g. account opening, funds management, bank statements and transfers and payments), as well as human resources and marketing.

Banks are required to apply more rigour and diligence when outsourcing basic works, given the more serious consequences if the arrangement results in non-delivery of services. For that reason, the outsourcing of basic works is generally not permitted, unless the bank first obtains permission from SAMA. The Outsourcing Rules contain detailed requirements about what must be addressed in outsourcing contracts for basic works, and these are primarily aimed at reducing the potential harm that could result from outsourcing these core tasks and responsibilities.

Non-basic Works

In contrast, non-basic works include services that are common to many businesses, and where outsourcing does not pose serious risk to customers. Examples include cleaning, printing and postal functions. Non-basic works may be assigned to third party service providers without first obtaining confirmation of no objection from SAMA.

Traditionally, banks would assign many non-basic works to third party service providers as a matter of course, and this may not have been considered ‘outsourcing’. Despite this, there may be implications for the outsourcing of such works in the Outsourcing Rules, so agreements relating to such works still need to be reviewed for compliance.

“The objective of the Outsourcing Rules is to provide guidance to banks on how to arrange outsourcing, while remaining compliant with the obligations under their banking licences.”

Risk evaluation and management

The Outsourcing Rules require senior management within banks to ensure that risks for existing and potential outsourcing agreements are considered and addressed. For the assignment of basic works, a thorough risk evaluation needs to be undertaken for all new contracts and contract renewals. For non-basic works, a thorough review is only required where there are substantive changes to the deliverables under an outsourcing arrangement.

Banks must properly investigate a service provider’s ability to undertake the contemplated services. Once a service provider is appointed, there is an obligation on the bank to monitor the service provider’s performance to ensure that the work is being done in accordance with the bank’s requirements.

Outsourcing contracts

The Outsourcing Rules require banks to put in place comprehensive outsourcing contracts with service providers. These contracts need to address a variety of requirements, including scope of work, service levels and performance requirements, control and audit procedures, business continuity, pricing, confidentiality and privacy, information security, effects of breach and dispute resolution. The Outsourcing Rules indicate that it is preferable for governing law and jurisdiction of outsourcing contracts be that of Saudi Arabia.

There is a requirement for outsourcing contracts to restrict service providers from sub-contracting any of the subject services without the prior consent of the banks, and subject to obtaining prior confirmation of no objection from SAMA.

Where customer data or financial statements are to be made available to a service provider in performance of outsourced services, it is necessary to ensure that the contractual arrangement reflects the confidentiality obligations set out in the Banking Control Law, and in other regulations and instructions that SAMA may have issued. It is also necessary to ensure that suitable measures are implemented to protect customer data and financial information in the course of performance of the outsourced services. These measures can include, for example, obligations requiring the adoption of isolation procedures restricting access to such information on a need-to-know basis, and obligations to have individuals involved in delivery of such services enter non-disclosure agreements.

Contracts for basic works need to make clear that SAMA has the right to obtain accounting documents and records relating to the assignment. Additionally, service providers located outside the Kingdom need to confirm that there are no statutory and control restrictions in their own jurisdictions that might impact on

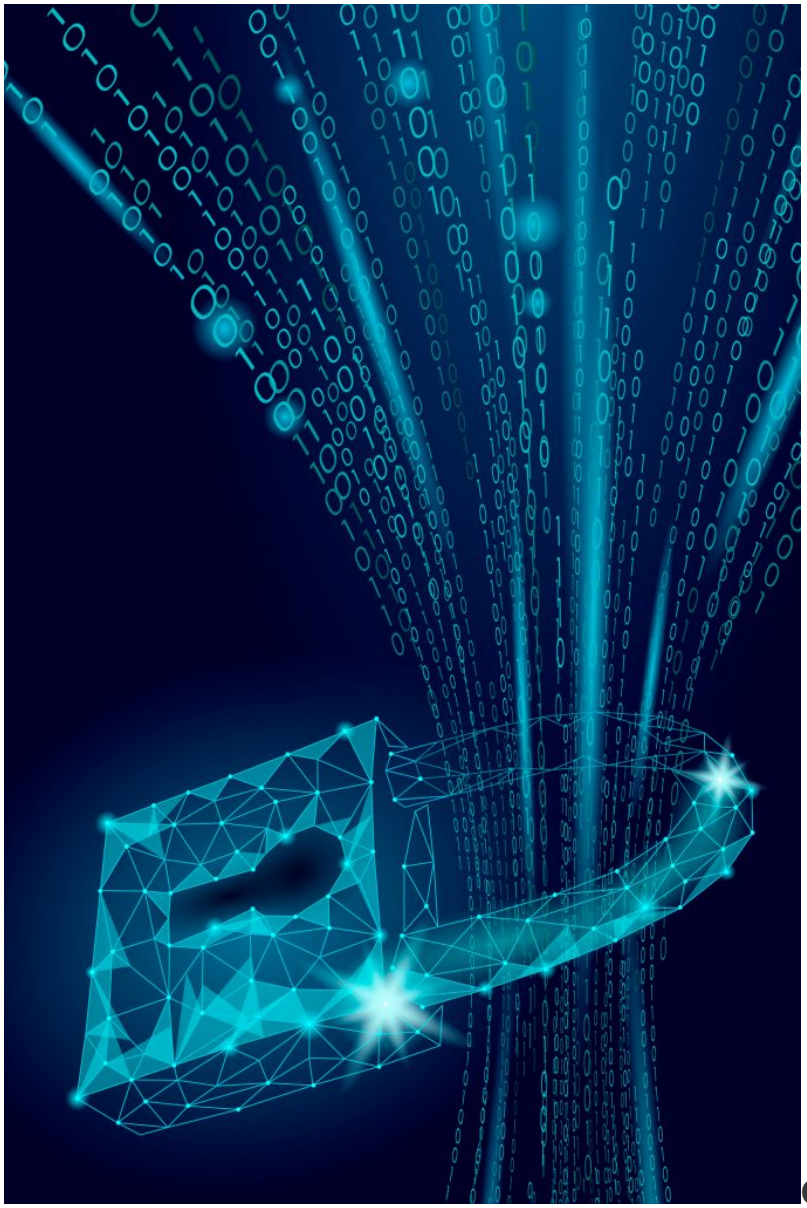
the unrestricted right of access to information that SAMA has under the Outsourcing Rules and the Banking Control Law.

Outsourcing contracts need to provide for the possibility of renewal, renegotiation, and termination of the contract, and early exit so that the bank can retain control over the subject services if it is necessary in the circumstances.

Business continuity

Outsourcing has the potential to cause interruptions or outages to banking services. Business continuity is very important for banks, particularly in terms of continuity of information technology services. The Outsourcing Rules require banks to have a plan in place to ensure business continuity if the outsourced service is disrupted. This can either be a plan for the bank to perform the function itself, or to have an alternate service provider ready to undertake the services on short notice. The Outsourcing Rules place an obligation on banks to inform SAMA of problems or disruptions that arise due to outsourcing arrangements.

In line with SAMA’s Business Continuity Management Framework (issued in 2017), banks need to have a business continuity strategy, and a business line responsible for implementing, monitoring and evaluating the strategy. An information technology disaster recovery plan is required as a key component of business continuity; it applies whether or not information technology services are outsourced. The Business Continuity Management Framework outlines how to develop and implement a business continuity strategy in more detail.



Cyber security considerations

The SAMA Cyber Security Framework (issued in 2017, and discussed in a separate Law Update article) acknowledges that banks will need to engage with third party service providers (including information technology services providers, cloud computing service providers, technology vendors and governmental agencies) in order to deliver their services. If such engagements do not respect the types of cyber security mechanisms that the banks have implemented, then they could result in cyber security risks. With this in mind, the Cyber Security Framework introduces expectations with regard to cyber security and the engagement of third parties. These can be broadly categorised as contract and vendor management considerations, outsourcing considerations and cloud computing considerations. It is essential that the cyber security obligations applying to banks pursuant to their implementation of SAMA's Cyber Security Framework are addressed when considering outsourcing arrangements, and when preparing associated outsourcing contracts.

Conclusion

Banks operating in Saudi Arabia need to be aware of the Outsourcing Rules. This is to ensure that they

remain compliant from a regulatory perspective, but also to ensure that the outsourcing of certain business operations does not result in damage to their customers, or to their own operation, reputations and profitability.

The risks are greater when banks outsource their core functions, and SAMA's Outsourcing Rules imposes greater obligations and restrictions on that type of outsourcing as a result.

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises on issues relating to technology contracting in the financial services sector. For further information please contact Nick O'Connell, Partner (n.oconnell@tamimi.com) or Amy Land-Pejoska, Associate (a.pejoska@tamimi.com).