UAE Central Bank Outsourcing Regulations: A Technology Perspective

Martin Hayward - Head of Digital & Data - Digital & Data
- Dubai International Financial Centre

With the announcement by the UAE Central Bank ("UAECB") of its new Outsourcing Regulations for Banks and accompanying Standards (Circular 14/2021 dated 31/05/2021, (together the "Regulations"), banks will need to take a closer and more detailed look at their outsourcing arrangements.

The Regulations cover all forms of outsourcing from business process (BPO) outsourcing of functions like HR or payroll to IT outsourcing. The definition of "outsourcing" is very broad (covering both external and intra-bank arrangements): "*an agreement with another party either within or outside the UAE, including a party related to the bank, to perform on a continuing basis an activity which currently is, or could be, undertaken by the bank itself*.

As a technology lawyer, the impact of the Regulations on IT outsourcing at a time of accelerating bank digitalisation and the growth of fintech offerings that enable banks to rapidly roll-out outsourced technology, usually cloud based, to deliver key bank functions (including compliance requirements) is especially interesting. We are at the start of a Middle East digital banking journey with challenger banks coming online. At a time when the regional banking market is combating significant disruption, these new regulations across the region are both timely and challenging as banks seek to balance the adoption of new technologies with increasing regulatory requirements. As the UAECB states in the Regulations: "*A key principle underpinning this Regulation is that a bank's outsourcing arrangements should not impair the bank's ability to fulfil its obligations to customers and to the Central Bank . . .*" The need for proactive, comprehensive, risk management has never been greater.

The approach banks are taking to outsourcing is also changing, based on the greater access to new,

disruptive, technologies. Where, previously, a bank would contract with a prime IT contractor who would take full responsibility for the delivery of a complete, “turnkey” outsourced solution, banks are now contracting with multiple technology vendors to cover multiple requirements. Banks will often contract with a systems integrator to integrate all these various technology deliverables. Banks will need to consider if the adoption of any new technology will constitute the outsourcing of a particular bank function and, if so, whether this would be considered material, or simply the technological enablement of a particular bank function with the bank retaining control of the function’s operation.

It is important to note that these Regulations are not introducing completely new concepts. The UAECB ‘s Regulations and Standards covering Risk Management and Operational Risk Management (Risk Management Regulations) have long been in place and the new Regulations need to be read in conjunction with these regulations. It also follows the recent issuance of the UAECB Consumer Protection Regulations and Standards. [link to ATCO article] It should also be noted that the financial freezones, Dubai International Financial Centre (DIFC) and Abu Dhabi Global Market (ADGM) have similar regulatory requirements in place. The Regulations apply to all banks in the UAE (excluding the DIFC and ADGM). For UAE banks, the Regulations apply group-wide and cover international subsidiaries and affiliates.

The Regulations cover all parts of the outsourcing lifecycle, from identifying the right outsourcing service provider, to contracting with them, maintaining a risk management and governance process throughout the outsourcing period and then managing any exit or migration away from the outsourcing service provider. Key functions of the bank from procurement through legal and compliance to internal audit need to be involved in the process in addition to the operational teams managing the day-to-day engagement with the outsourcing service provider.

Procurement

Bank procurement processes need to build in the Regulations’ requirements. Procurement policies need to cover the procurement aspects in the Regulations. An appropriate and documented due diligence review process is required to ensure that the selected outsourcing service provider can meet the bank’s requirements (including the outsourcing service provider financial capacity requirements). This may be particularly challenging as banks look to the fintech start-up ecosystem for new products and technologies. Procurement teams also need to guard against vendor lock-in in their choice of outsourcing service provider and also continuously monitor the aggregate outsourcing risk the bank is taking on.

Governance and Risk Management.

The Regulations emphasize that banks remain fully responsible for the risks arising from any process or activity they outsource and for ensuring that they remain compliant with all relevant laws and regulations applicable to their outsourced activities. As a result, banks need the following:

- A process for determining the materiality of any outsourcing activities – this is particularly important as banks must obtain a prior notice of non-objection for the outsourcing of any material activity from the UAECB. The Regulations note that the outsourcing of core banking activities such as risk management, compliance, internal audit and the management of risk taking functions such as investment and treasury management will be challenging and generally not permitted (although any outsourcing arrangement will be considered on its individual merits). The Regulations highlight the need to engage proactively, and early in the procurement process, with the UAECB in relation to a material outsourcing;
- Board-approved outsourcing policies and procedures (as part of the bank’s risk governance framework (required under the UAECB Risk Management Regulations)) to assess, measure, monitor and report (to

the bank's board or specific board outsourcing committee) on any risk associated with ongoing and potential outsourcing activities (at a group-wide level – including services the bank provides or delivers to group members) and identify potential conflicts of interest;
- Allocation of roles and responsibilities within the bank for managing the outsourcing arrangement (including the role of the bank's internal audit function which will need to regularly assess the effectiveness of the bank's outsourcing arrangements);
- Coverage of the outsourced activity in the bank's disaster recovery and business continuity plans (DRBCP) and contractual commitments from the bank's outsourcing service providers to implement any bank DRBCP and also have their own in place.
- Outsourcing service providers must have demonstrable and appropriate levels of information security, risk management and service delivery in place (with the contracts with these providers covering these areas in detail;
- Banks must maintain a comprehensive and up-to-date register of all outsourcing arrangements (both material and non-material). The register must cover full details of the outsourcing arrangement, whether the arrangement is considered "material" and whether the arrangement involves any Confidential Data. "Confidential Data" is defined in the Regulations as: "*Account or other data relating to a Bank customer, who is or can be identified from the confidential fata, or from the confidential data in conjunction with other information that is on, or is likely to come into , the possession of a person or organization that is granted access to the confidential data.*".

Data Protection

The recent UAECB Consumer Protection Regulations and Standards dealt, in detail, with data protection. The Regulations reiterate the need for banks to continue to meet their legal and regulatory obligations in relation to the management and processing of data, even when outsourced. The key issues for banks include:

- retaining ownership in all data (including Confidential Data) provided to an outsourcing service provider and ensuring that the bank and their customers can effectively exercise rights and duties over such data;
- ensuring that outsourcing service providers flow down their commitments to subcontractors and that the subcontractors are fully compliant with the Regulations;
- requiring outsourcing service providers to keep data secure.

With data often held in cloud storage and banks adopting new and emerging technologies, such as blockchain and artificial intelligence, banks need to carefully analyse whether they can continue to meet their regulatory requirements in relation to data. The banks' contracts with outsourcing service providers will need to include detailed provisions covering these requirements (see below).

Outsourcing Agreements

It is mandatory for banks to have formal written outsourcing arrangements in place with outsourcing service providers that are robust and detailed. The Regulations set out the required minimum content of these outsourcing arrangements. The scope of the outsourcing and the respective rights and responsibilities of the parties need to be clearly set out in addition to pricing and fee structure, performance requirements, dispute resolution governance, reporting and monitoring. Term, termination, liability and insurance provisions need careful attention.

In particular, these outsourcing arrangements need to cover the following:

- effectively apply the banks' policies and procedures to the outsourcing arrangement. Banks need to ensure that they have fully captured their requirements in their policies and procedures and secure the outsourcing service provider's compliance with these policies and procedures;
- ensure the bank and its customers retain full ownership of, and unfettered access, to their data (both during the outsourcing arrangement and on termination), particularly where outsourcing service providers are seeking to use customer data for data analytics purposes. As noted above, banks need to understand the potential challenges to meeting these regulatory requirements based on the types of technology they adopt. Banks also need detailed exit and migration provisions covering the recovery of data on termination;
- the protection (including destruction) of data. The Regulations reference the need to specifically establish standards for data protection, including any nationally recognised information assurance standards (for example, applying the UAE Information Assurance Standards, a part of the UAE's National Cyber Security Strategy). The Regulations also limit any provision of Confidential Data to third parties by outsourcing service providers (or their subcontractors) without specific bank (or customer) authorisation. Banks need to build in these authorisations with outsourcing service providers and also, through their terms and conditions, with their customers;
- data breach notification requirements;
- the parameters of any outsourcing service provider subcontracting arrangement need to be set out in detail; and
- audit provisions are essential, covering both bank and UAECB (and its agents') unrestricted access to the outsourcing service provider. This includes the ability for the UAECB to directly request data from the outsourcing service provider.

Outsourcing outside the UAE

The Regulations place certain limitations on outsourcing outside the UAE. These include:

- ensuring that the Master System of Record, including all Confidential Data, is maintained and stored within the UAE. The "Master System of Record" is defined in the Regulations as: "*the collection of all data, including Confidential Data, required to conduct all core activities of a Bank, including the provision of services to clients, managing all risk, and complying with all legal and regulatory requirements*.". Branches of foreign banks can, with UAECB approval, meet these requirements by retaining a daily updated copy of the Master System of Record within the UAE.
- Confidential Data remaining within the UAE, except where UAECB and customer approval has been secured. Furthermore, banks cannot share Confidential Data with service providers located in jurisdictions that cannot provide the same level of security for Confidential Data that would apply in the UAE. The Regulations do not detail what level of security applies in the UAE so banks will need to make their own determination based on industry practice and standards. Banks must also ensure that data is not stored in a jurisdiction that restricts or limits access to data for supervisory purposes. As with security of Confidential Data, banks will need to make their own assessment on such jurisdictions;
- data held outside the UAE must be available at all times to the bank and the UAECB and bank staff must be trained to manage the outsourcing of data (including outside the UAE);
- banks must consider, and outsourcing agreements need to reflect, the potential for changes in economic, political, social, legal or regulatory conditions that could affect the ability of a service provider outside the UAE to meet the terms of the agreement. The risk needs to managed both at the procurement stage with the careful selection of service provider, via the contract (e.g. with regulatory change provisions) and operationally (including through good business continuity planning).

Banks need to think carefully before outsourcing outside the UAE with the additional requirements to manage operational, legal and reputational risk and put in place policies and procedures to manage (and mitigate) these risks. Banks also need to fully understand how the technologies they are using use and

transfer data, what data is involved and in what form (e.g. anonymised, encrypted, etc.) and where it goes.

Reporting

The Regulation introduces new reporting requirements for banks. These include:

- regular reporting on outsourcing arrangements in a format and frequency prescribed by the UAECB;
- providing any specific information the UAECB requests on its outsourcing arrangements;
- providing the UAECB with a copy of the bank's outsourcing register on request;
- notifying the UAECB immediately when the bank becomes aware of a material breach of any oursourcing agreement or any development in relation to a material outsourced activity that is or will have a significant impact on the bank's operations, reputation or financial condition.

Banks will need to ensure that they have processes and procedures established to meet these reporting requirements and that these reporting requirements are covered in their contracts with its outsourcing service providers to ensure that theycan extract the right data in the right format to meet their regulatory requirements.

Violations of the Regulations can trigger supervisory action and/ administrative and financial sanctions by the UAECB. The UAECB can also require a bank to terminate an outsourcing arrangement where the arrangement is found to be no longer compliant with the Regulations or presents undue risks to the bank, the security of Confidential Data or the UAE financial system. Banks need to cover this in their termination provisions with their outsourcing service providers in addition to flowing the financial risk of supervisory action and sanctions down to outsourcing service providers.

Islamic banking

Any outsourcing activities by banks offering Islamic financial services need to ensure that Shari'iah rules and principles are observed.

Timeline for implementation

All outsourcing arrangements concluded or renewed after this Regulation came into force on 14 July 2021 (one month after being published in the Official Gazette) must comply fully with these regulations. All outsourcing agreements concluded prior to the Regulations coming into force must be amended so that they fully comply with the Regulations by 31 December 2023. For existing outsourcing agreements, banks should be engaging as soon as possible with their outsourcing service providers to socialise the new Regulations and start the discussion on any required amendments to their outsourcing arrangements.

Al Tamimi's Digital & Data team regularly advises UAE financial services clients on technology, data protection and cybersecurity matters. For more information on how we can help, please contact Martin Hayward.