United Arab Emirates

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Outsourcing Standards for Banks

Contents

1 Introduction

These Standards form part of the Outsourcing Regulation for Banks (Circular No. 14/2021). All Banks are required to comply with these Standards, which expand on the Regulation and will be enforced by the Central Bank.

Banks outsource activities for a variety of business reasons. However, there are risks associated with outsourcing and these risks must be appropriately managed to ensure that the Bank is able to meet its financial and service obligations, regardless of whether a business activity is undertaken by the Bank itself or outsourced.

A Bank's Board is in ultimate control of the Bank and accordingly, remains responsible for any business activities which have been outsourced. The Board is responsible for ensuring that all risks related to outsourcing are identified and that appropriate policies and procedures are in place to manage those risks.

The Standards follow the structure of the Regulation, with each article corresponding to the specific article in the Regulation.

2 Governance and risk management

2.1 Risk governance framework

Banks must have an appropriate risk governance framework in place in accordance with the Central Bank's risk management Regulations and Standards. This risk governance framework must be comprehensive and include within its scope any outsourced business activities and specifically address the additional risks that arise when a business activity is outsourced, including but not limited to:

1. Operational risk arising from inadequate processes or systems, insufficient or inadequately trained or supervised staff, fraud or error on the part of the outsourcing service provider;

2. Compliance risk arising from failure by the Outsourcing Service Provider to adhere to laws and regulations or the Bank's policies, standards or codes of conduct;

3. Vendor lock-in and business continuity risk, arising from inadequate contractual and practical arrangements to ensure an outsourced business activity can be either transferred to another service provider or the Bank itself without undue delay, or discontinued without significantly disrupting the Bank's operations, or its ability to manage risks;

4. Concentration risk arising from relying on the same outsourcing service provider for multiple outsourcing arrangements, or from reliance by different outsourcing providers on the same subcontractor;

5. Governance and internal control risk arising from excessive outsourcing as a whole, in a specific domain or department, or overreliance on third parties in the operation of the business;

6. The aggregate risk from all outsourcing arrangements and the marginal risk of any proposed outsourcing arrangement.

2.2 Policies and procedures for the assessment and approval of outsourcing material business activities

Banks must have policies and procedures to ensure compliance with the applicable regulations and standards and to ensure the following has been achieved prior to outsourcing a business activity:

1. The Board or a committee of the Board has been adequately informed and has approved the outsourcing arrangement, as required;

2. An appropriate due diligence review has been undertaken of the selected outsourcing service provider addressing factors including, but not limited to:
    a. Ability, including financial capacity, to meet the requirements of the arrangement and deliver the service reliably;
    b. Experience with similar agreements and services;
    c. Governance, internal control, internal audit, reporting and monitoring capabilities;
    d. Security, including cyber security;
    e. Staffing, including employee qualifications and expertise; and
    f. Country risk factors and legal environment where applicable.
3. Procedures are implemented to monitor performance under the outsourcing agreement;
4. Appropriate provisions for business continuity and disaster recovery are in place, including contingency plans to bring the outsourced function back in-house should the need arise, or the identification of alternative outsourcing service providers.

2.3 Materiality of outsourcing arrangements

Banks must consider at least the following when determining the materiality of an outsourcing agreement:

1. The impact on the Bank's ability to manage and control its risks;
2. The impact on the Bank's performance and control over its performance;
3. The impact of an outsourcing service provider's failure to deliver the service as per the agreement, including failures to mitigate risks or to operate in a safe and prudent manner;
4. The impact on the Bank's ability to comply with its legal and regulatory requirements;
5. The nature of the data shared as part of the outsourcing agreement.

3 Outsourcing register

The aim of the outsourcing register is to provide both internal parties as well as external parties, such as external auditors or the Central Bank, with a comprehensive overview of a Bank's outsourcing. In order to meet these objectives, an outsourcing register should be established and maintained that is:

1. Comprehensive;
2. Up to date;
3. Allows to distinguish between material and non-material outsourcing;
4. Allows to distinguish between varying levels of risk;
5. Specifies whether data is being shared and if so, what type of data.

4 Data protection

Banks must ensure that outsourcing agreements provide for at least the same degree of data protection that would apply if they performed the outsourced activity themselves. Banks must therefore establish adequate policies and procedures, and make all necessary steps to ensure data integrity, confidentiality, and accessibility. At a minimum, these policies and measures must address, both for digital and physical access, the following:

1. Access rights management, including but not limited to policies for granting and revoking access rights and a periodic review of user privileges;
2. Protection against digital and physical attacks;
3. Protection of the integrity of data;
4. Audit trails;
5. Measures to detect, react to, and recover from data security incidents.

5 Outsourcing agreements

5.1 Required minimum content

Outsourcing agreements should establish a degree of certainty with regard to at least the following:

1. Scope of the arrangement, the services to be supplied, and the rights and responsibilities of all parties involved;
2. Pricing and fee structure;
3. Service level and performance requirements;
4. Governance, security, audit, reporting and monitoring procedures;
5. Business continuity and disaster recovery management;
6. Confidentiality, privacy and security of information;
7. Default arrangements and termination provisions, addressing also premature termination for any reason;
8. Liability, indemnity and insurance;
9. Compliance with anti-money laundering and combatting the financing of terrorism laws and regulations;
10. Start and end date of the agreement, and provisions for reviewing, renewing or terminating the agreement;
11. Dispute resolution arrangements, including designation of the legal jurisdictions that will apply;
12. Whether subcontracting is allowed and under which conditions;
13. Protection of Bank's and its customers' data handled as part of the agreement;
14. Requirements for the outsourcing service provider to notify the Bank without undue delay of any breach of the Bank's data, in particular breaches of Confidential Data; and
15. Right of the Central Bank, and any agent appointed by the Central Bank, to conduct on-site visits at the outsourcing service provider and obtain any data or information from the outsourcing service provider required for supervisory purposes.

5.2 Access to the outsourcing service provider by the Central Bank

The Central Bank requires the same access for supervisory purposes to business activities that have been outsourced as it would have if the business activity were undertaken by the Bank itself.

Normally, the Central Bank will obtain any information it requires from the Bank. However, each outsourcing agreement must include explicit provisions requiring the outsourcing service provider to provide directly to the Central Bank, upon request, any data or information the Central Bank deems necessary for supervisory purposes.

In addition, outsourcing agreements must provide that the Central Bank and any agent appointed by the Central Bank, may, if deemed necessary, conduct on-site visits at the outsourcing service provider with right of access to data and staff as if the activity were undertaken by the Bank.

6 Outsourcing outside the UAE

Banks must consider the risks associated with outsourcing business activities to outsourcing service providers who are themselves or whose subcontractors are located in other jurisdictions, and manage or mitigate these risks.

7 Internal audit and compliance

Outsourced activities must remain fully in scope of the internal audit and compliance responsibilities and should follow the same risk-based approach as for activities performed by the Bank itself, while taking into account the additional risks arising from outsourcing these activities.

The internal audit function of the Bank must be able to obtain all information necessary to provide assurance to the Board, and must be able to demand an extension of the scope of audits performed by third parties where necessary.

8 Non-objection by the Central Bank

Prior to entering into an agreement to outsource a material business activity, Banks must obtain the non-objection of the Central Bank. When requesting the non-objection, Banks must provide the Central Bank with the following at a minimum:

1. A brief explanation of the business activity to be outsourced;
2. A summary of the materiality assessment;
3. A summary of the risk assessment;
4. A summary of the due diligence performed and its outcome;
5. A confirmation of the agreement of the internal audit function and the compliance function;
6. An overview of any closely related outsourcing agreements;
7. Confirmation of compliance with the requirements of the Outsourcing for Banks Regulation;
8. Evidence of the approval of the proposed outsourcing by the Board or Board committee.

The Central Bank will either grant the non-objection or request further information. Banks are encouraged to discuss their material outsourcing plans early on and coordinate with the Central Bank to avoid the non-objection process delaying the outsourcing.

9 Reporting requirements

Banks must regularly report to the Central Bank on their outsourcing arrangements in the format and frequency prescribed by the Central Bank.

10 Islamic Banking

A bank offering Islamic financial services must ensure that its Sharī'ah governance system explicitly considers Sharī'ah rules and principles with respect to any outsourced activities. The rules and principles are those that would apply if the bank itself performed the activity. A bank offering Islamic financial services must also ensure that its policies and procedures for the review and approval of any proposed outsourcing arrangements explicitly address the risk that Outsourcing Service Providers may be unfamiliar with requirements relating to Sharī'ah rules and principles.

Ensuring Shari'ah compliance for individual products requires that the entire product cycle takes into account Shari'ah rules and principles, even if some activities related to specific products are outsourced, so a bank offering Islamic financial services must include in its outsourcing agreements any necessary measures to mitigate the operational and reputational risks of Shari'ah non-compliance.