MONEY CHANGERS RISK MANAGEMENT MODULE

MODULE:	RM (Risk Management)

Table of Contents

			Date Last Changed
RM-A	**Introduction**		
	RM-A.1	Purpose	01/2011
	RM-A.2	Module History	01/2021
RM-B	**Scope of Application**		
	RM-B.1	Scope of Application	10/2010
RM-1	**General Requirements**		
	RM-1.1	Risk Management	10/2010
	RM-1.2	Counterparty Risk	10/2010
	RM-1.3	Liquidity Risk	10/2010
	RM-1.4	Market Risk	10/2010
	RM-1.5	Operational Risk	01/2021
RM-2	**Outsourcing of Risk**		
	RM-2.1	Outsourcing of Risk	10/2017
	RM-2.2	Outsourcing Agreement	10/2017
	RM-2.3	Intragroup Outsourcing	10/2017
	RM-2.4	Internal Audit Outsourcing	10/2010

RM-A.1 Purpose

Executive Summary

RM-A.1.1 This Module contains requirements relating to the management of risk by licencees. It expands on certain high level requirements contained in other Modules. In particular, Section AU-2.6 of Module AU (Authorisation) specifies requirements regarding systems and controls that have to be met as a license condition; Principle 10 of the Principles of Business (ref. PB-1.10) requires licencees to have systems and controls sufficient to manage the level of risk inherent in their business; and Module HC (High-level Controls) specifies various requirements relating to the role and composition of Boards, and related high-level controls.

RM-A.1.2 This Module obliges licensees to recognise the range of risks that they face and the need to manage these effectively. Their risk management framework is expected to have the resources and tools to identify, monitor and control all material risks. The adequacy of a licensee's risk management framework is subject to the scale and complexity of its operations, however. In demonstrating compliance with certain Rules, licensees with very simple operational structures and business activities may need to implement less extensive or sophisticated risk management systems, compared to licensees with a complex and/or extensive customer base or operations.

Legal Basis

RM-A.1.3 **This Module contains the Central Bank of Bahrain's ('CBB') Directive (as amended from time to time) regarding Risk Management requirements applicable to licensees, and is issued under the powers available to the CBB under Article 38 of the Central Bank of Bahrain and Financial Institutions Law 2006 ('CBB Law'). Requirements regarding Money Changer Licensees are also included in the Regulation Organising Money Changing Business, issued in 1994 and included in this Module.**

RM-A.1.4 For an explanation of the CBB's rule-making powers and different regulatory instruments, see section UG-1.1.

RM-A.2 Module History

Evolution of the Module

RM-A.2.1 This Module was first issued in October 2010. Any material changes that have subsequently been made to this Module are annotated with the calendar quarter date in which the change was made: Chapter UG-3 provides further details on Rulebook maintenance and version control.

RM-A.2.2 A list of recent changes made to this Module is provided below:

Module Ref.	Change Date	Description of Changes
RM-A.1.3	01/2011	Clarified legal basis.
RM-2.1.2	10/2017	Amended Paragraph to allow the utilization of cloud services.
RM-2.1.4A	10/2017	Added a new Paragraph on outsourcing requirements.
RM-2.1.7	10/2017	Amended Paragraph.
RM-2.1.9	10/2017	Amended Paragraph.
RM-2.1.11	10/2017	Amended Paragraph.
RM-2.1.13	10/2017	Added a new Paragraph on outsourcing.
RM-2.1.15	10/2017	Amended Paragraph.
RM-2.2.9	10/2017	Amended Paragraph.
RM-2.2.15	10/2017	Amended Paragraph.
RM-2.2.16	10/2017	Added a new Paragraph on security measures related to cloud services.
RM-2.3.2	10/2017	Amended Paragraph.
RM-1.5.5	01/2021	Added a new Paragraph on electronic fraud.
RM-1.5.6	01/2021	Added a new Paragraph on electronic fraud awareness.

Superseded Requirements

RM-A.2.3 This Module does not replace any regulations or circulars in force prior to month year.

Document Ref.	Date of Issue	Module Ref.	Document Subject

MODULE	RM:	Risk Management
CHAPTER	RM-B:	Scope of Application

RM-B.1 Scope of Application

RM-B.1.1 The content of this Module applies to all Money Changer licensees authorised in the Kingdom, thereafter referred to in this Module as licensees.

MODULE	RM:	Risk Management
CHAPTER	RM-1:	General Requirements

RM-1.1 Risk Management

Board of Directors' Responsibility

RM-1.1.1 **The Board of Directors of licensees must take responsibility for the establishment of an adequate and effective framework for identifying, monitoring and managing risks across all its operations.**

RM-1.1.2 The CBB expects the Board to be able to demonstrate that it provides suitable oversight and establishes, in relation to all the risks the licencee is exposed to, a risk management framework that includes setting and monitoring policies, systems, tools and controls.

RM-1.1.3 Although authority for the management of a firm's risks is likely to be delegated, to some degree, to individuals at all levels of the organisation, the overall responsibility for this activity should not be delegated from its governing body and relevant senior managers.

RM-1.1.4 A licencees's failure to establish, in the opinion of the CBB, an adequate risk management framework will result in it being in breach of Condition 6 of the Licensing Conditions of Section AU-2.6. This failure may result in the CBB withdrawing or imposing restrictions on the licensee, or the licensee being required to inject more capital.

RM-1.1.5 **The Board of Directors must also ensure that there is adequate documentation of the licensee's risk management framework.**

Systems and Controls

RM-1.1.6 **The risk management framework of licensees must provide for the establishment and maintenance of effective systems and controls as are appropriate to their business, so as to identify, measure, monitor and manage risks.**

RM-1.1.7 An effective framework for risk management should include systems to identify, measure, monitor and control all major risks on an on-going basis. The risk management systems should be approved and periodically reviewed by the Board as outlined in HC-1.1.5.

RM-1.1 Risk Management (continued)

Systems and Controls (continued)

RM-1.1.8 **The systems and controls required by Paragraph RM-1.1.6 must be proportionate to the nature, scale and complexity of the firm's activities.**

RM-1.1.9 The processes and systems required must enable the licensee to identify the major sources of risk to its ability to meet its liabilities as they fall due, which include but are not limited to the following:

(a) Counterparty Risk;
(b) Liquidity Risk;
(c) Market Risk; and
(d) Operational Risk.

RM-1.2 Counterparty Risk

RM-1.2.1 Licensees must adequately document the necessary policies and procedures for identifying, measuring, monitoring and controlling counterparty risk. This policy must be approved and regularly reviewed by the Board of Directors of the licensee.

RM-1.2.2 Among other things, the licensee's policies and procedures must identify the limits it applies to counterparties, how it monitors movements in counterparty risk and how it mitigates loss in the event of counterparty failure.

RM-1.3 Liquidity Risk

RM-1.3.1 Licensees must maintain a liquidity risk policy for the management of liquidity risk, which is appropriate to the nature, scale and complexity of its activities. This policy must be approved and regularly reviewed by the Board of Directors of the licensee.

RM-1.3.2 Among other things, the licensee's liquidity risk policy must identify the limits it applies, how it monitors movements in risk and how it mitigates loss in the event of unexpected liquidity events.

RM-1.4 Market Risk

RM-1.4.1 Licensees must document their framework for the proactive management of market risk. This policy must be approved and regularly reviewed by the Board of Directors of the licensee.

RM-1.5 Operational Risk

RM-1.5.1 **Licensees must document their framework for the proactive management of operational risk. This policy must be approved and regularly reviewed by the Board of Directors of the licensee.**

RM-1.5.2 **Licensees must consider the impact of operational risks on their financial resources and solvency.**

RM-1.5.3 **Licensees' business continuity planning, risk identification and reporting must cover reasonably foreseeable external events and their likely impact on the licensee and its business portfolio.**

RM-1.5.4 Business continuity management includes policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption. Its purpose is to minimise the operational, financial, legal, reputational and other material consequences arising from a disruption. Effective business continuity management concentrates on the impact, as opposed to the source, of the disruption, which affords financial industry participants and financial authorities greater flexibility to address a broad range of disruptions. At the same time, however, licencees cannot ignore the nature of risks to which they are exposed.

Electronic Frauds

RM-1.5.5 **Licensees must implement enhanced fraud monitoring of movements in customers' accounts to guard against electronic frauds using various tools and measures, such as limits in value, volume and velocity.**

RM-1.5.6 **Licensees must have in place customer awareness communications, pre and post registration process, using video calls, short videos or pop-up messages, to alert and warn natural persons using online channels or applications about the risk of electronic frauds, and emphasise the need to secure their personal credentials and not share them with anyone, online or offline.**

RM-2.1 Outsourcing of Risk

RM-2.1.1 **Licensees must identify all material outsourcing contracts and ensure that the risks associated with such contracts are adequately controlled. In particular, licensees must comply with the specific requirements set out in this Chapter.**

RM-2.1.2 **Licensees may not outsource their core business activities to a third party.**

RM-2.1.3 Outsourcing means an arrangement whereby a third party performs on behalf of a licensee an activity that was previously undertaken by the licensee itself (or in the case of a new activity, one which ordinarily would have been performed internally by the licensee). Examples of services that are typically outsourced include data processing, cloud services, customer call centres and back-office related activities.

RM-2.1.4 For purposes of Paragraph RM-2.1.1, a contract is 'material' where, if it failed in any way, it would pose significant risks to the on-going operations of a licensee, its reputation and/or the quality of service provided to its customers. For instance, the outsourcing of all or a substantial part of functions such as customer sales and relationship management, settlements and processing, IT and data processing and financial control, would normally be considered "material". Management should carefully consider whether a proposed outsourcing arrangement falls under this Module's definition of "material". If in doubt, management should consult with the CBB.

RM-2.1.4A For outsourcing services that are not considered material outsourcing arrangements, licenses must submit a written notification to the CBB before committing to the new outsourcing arrangement.

RM-2.1.5 **Licensees must retain ultimate responsibility for functions or activities that are outsourced. In particular, licensees must ensure that they continue to meet all their regulatory obligations with respect to outsourced activities.**

RM-2.1.6 **Licensees must not contract out their regulatory obligations and must take reasonable care to supervise the discharge of outsourced functions, if any.**

Supervisory Approach

RM-2.1.7 **Licensees must seek the CBB's prior written approval before committing to a new material outsourcing arrangement.**

RM-2.1 Outsourcing of Risk (continued)

Supervisory Approach (continued)

RM-2.1.8 **The prior approval request in Paragraph RM-2.1.7 must:**
(a) Be made in writing to the licensee's normal supervisory contact;
(b) Contain sufficient detail to demonstrate that relevant issues raised in this Chapter have been addressed; and
(c) Be made at least 6 weeks before the licensee intends to commit to the arrangement.

RM-2.1.9 The CBB will review the information provided and provide a definitive response within a reasonable period of time of receiving the request for approval.

RM-2.1.10 **Once an activity has been outsourced, a licensee must continue to monitor the associated risks and the effectiveness of its mitigating controls.**

RM-2.1.11 **Licensees must immediately inform their normal supervisory contact at the CBB of any material problems encountered with an outsourcing provider. The CBB may direct the licensees to make alternative arrangements for the outsourced activity.**

RM-2.1.12 **The CBB requires ongoing access to the outsourced activity, which it may occasionally want to examine, through management meetings or on-site examinations.**

RM-2.1.13 The CBB reserves the right to require a licensee to terminate or make alternative outsourcing arrangements if, among other reasons, the confidentiality of its customer information was, or is likely to be, breached or the ability of the CBB to carry out its supervisory functions in view of the outsourcing arrangement cannot be assured or executed.

RM-2.1 Outsourcing of Risk (continued)

Supervisory Approach (continued)

RM-2.1.13 In negotiating its contract with a service provider, a licensee should have regard to:

(a) Reporting or notification requirements it may wish to impose on the service provider;

(b) Whether sufficient access will be available to its internal auditors, external auditors and to the CBB;

(c) Information ownership rights, confidentiality agreements and Chinese walls to protect customer and other information (including arrangements at the termination of the contract);

(d) The adequacy of any guarantees and indemnities;

(e) The extent to which the service provider must comply with the licensee's policies and procedures (covering, for example, information security)

(f) The extent to which a service provider will provide business continuity for outsourcing operations, and whether exclusive access to its resources is agreed;

(g) The need for continued availability of software following difficulty at a third party supplier; and

(h) The processes for making changes to the outsourcing arrangement (for example, changes in processing volumes, activities and other contractual terms) and the conditions under which the licensee or service provider can choose to change or terminate the outsourcing arrangement, such as where there is:

(i) A change of ownership or control (including insolvency or receivership) of the service provider or firm;

(ii) Significant change in the business operations (including sub-contracting) of the service provider or firm; or

(iii) Inadequate provision of services that may lead to the firm being unable to meet its regulatory obligations.

RM-2.1.14 **Licensees must maintain and regularly review contingency plans to enable them to set up alternative arrangements – with minimum disruption to business – should the outsourcing contract be suddenly terminated or the outsourcing provider fail. This may involve the identification of alternative outsourcing providers or the provision of the service in-house. These plans should consider how long the transition would take and what interim arrangements would apply.**

RM-2.1 Outsourcing of Risk (continued)

Supervisory Approach (continued)

RM-2.1.15 A licensee must nominate a relevant approved person within the licensee to handle the responsibility of the day-to-day relationship with the outsourcing provider and to ensure that relevant risks are addressed. The CBB should be informed of the designated individual as part of the request for prior approval required under Rule RM-2.1.7. Any subsequent replacement of such person must also be notified to the CBB.

RM-2.1.16 All material outsourcing arrangements by licensees must be the subject of a legally enforceable contract. Where the outsourcing provider interacts directly with a licensee's customers, the contract must – where relevant – reflect the licensee's own standards regarding customer care. Once an outsourcing agreement has been entered into, licensees must regularly review the suitability of the outsourcing provider and the on-going impact of the agreement on their risk profile and systems and controls framework.

MODULE	RM:	Risk Management
CHAPTER	RM-2:	Outsourcing of Risk

RM-2.2 Outsourcing Agreement

RM-2.2.1 **The activities to be outsourced and respective contractual liabilities and obligations of the outsourcing provider and licensee must be clearly specified in an outsourcing agreement. This agreement must – amongst other things – address the issues identified below in this Section.**

Control Over Outsourced Activities

RM-2.2.2 **The Board and management of licensees are held ultimately responsible by the CBB for the adequacy of systems and controls in outsourced activities. Licensees must therefore ensure they have adequate mechanisms for monitoring the performance of, and managing the relationship with, the outsourcing provider.**

RM-2.2.3 **Clear reporting and escalation mechanisms must be specified in the agreement.**

Customer Data Confidentiality

RM-2.2.4 **Licensees must ensure that outsourcing agreements comply with all applicable legal requirements regarding customer confidentiality.**

RM-2.2.5 **Licensees must ensure that the outsourcing provider implements adequate safeguards and procedures.**

RM-2.2.6 For the purposes of Paragraph RM-2.2.5, the implementation of adequate safeguards would include the proper segregation of customer data from those belonging to other customers of the outsourcing provider. Outsourcing providers should give suitable undertakings that the company and its staff will comply with all applicable confidentiality rules. Licensees should have contractual rights to take action against the service provider in the event of breach of confidentiality.

RM-2.2.7 **Licensees must ensure that they retain title under any outsourcing agreements for data, information and records that form part of the prudential records of the licensee.**

RM-2.2 Outsourcing Agreement (continued)

Access to Information

RM-2.2.8 Outsourcing agreements must ensure that the licensees' internal and external auditors have timely access to any relevant information they may require to fulfil their responsibilities. Such access must allow them to conduct on-site examinations of the outsourcing provider, if required.

RM-2.2.9 Licensees must also ensure that the CBB inspectors and appointed experts have timely access to any relevant information they may reasonably require to fulfil its responsibilities under the CBB Law. Such access must allow the CBB to conduct on-site examinations of the outsourcing provider, if required.

RM-2.2.10 The outsourcing provider must commit itself, in the outsourcing agreement, to informing the licensee of any developments that may have a material impact on its ability to meet its obligations. These may include, for example, relevant control weaknesses identified by the outsourcing provider's internal or external auditors, and material adverse developments in the financial performance of the outsourcing provider.

Business Continuity

RM-2.2.11 Licensees must ensure that service providers maintain, regularly review and test plans to ensure continuity in the provision of the outsourced service.

RM-2.2.12 Licensees must have an adequate understanding of the outsourcing provider's contingency arrangements, to understand the implications for the licensee's own contingency arrangements.

Termination

RM-2.2.13 Licensees must have a right to terminate the agreement should the outsourcing provider:

(a) Undergo a change of ownership (whether direct or indirect) that poses a potential conflict of interest;
(b) Becomes insolvent; or
(c) Goes into liquidation or administration.

RM-2.2 Outsourcing Agreement (continued)

Termination (continued)

RM-2.2.14 Termination under any other circumstances allowed under the agreement must give licensees a sufficient notice period in which they can effect a smooth transfer of the service to another provider or bring it back in-house.

RM-2.2.15 In the event of termination, for whatever reason, the agreement must provide for the return of all customer data – where required by licensees – or destruction of the records.

Cloud Services

RM-2.2.16 For the purpose of outsourcing of cloud services, licensees must ensure that, at a minimum, the following security measures are in place:

(a) Customer information must be encrypted and licensees must ensure that all encryption keys or similar forms of authentication are kept secure within the licensee's control;
(b) A secure audit trail must be maintained for all actions performed at the cloud services outsourcing provider;
(c) A comprehensive change management procedure must be developed to account for future changes to technology with adequate testing of such changes;
(d) The licensee's data must be logically segregated from other entities data at the outsourcing service provider's platform;
(e) The cloud service provider must provide information on measures taken at its platform to ensure adequate information security, data security and confidentiality, including but not limited to forms of protection available against unauthorized access and incident management process in cases of data breach or data loss; and
(f) The right to release customer information/data in case of foreign government/court orders must be the sole responsibility of the licensee, subject to the CBB Law.

RM-2.3 Intragroup Outsourcing

RM-2.3.1 As with outsourcing to non-group companies, the Board and management of licensees are held ultimately responsible by the CBB for the adequacy of systems and controls in activities outsourced to group companies.

RM-2.3.2 Licensees must obtain CBB's prior written approval before committing to a material intragroup outsourcing. The request for approval must be made in writing to the licensee's normal supervisory contact at least 6 weeks prior to committing to the outsourcing, and must set out a summary of the proposed outsourcing, its rationale, and an analysis of its associated risks and proposed mitigating controls. All other Rules in this Chapter apply to intragroup outsourcing.

RM-2.3.3 Licensees may not outsource their core business activities, including the internal audit function, to their group. The outsourcing of certain functions is subject to the provisions of Modules RM (Risk Management), HC (High-Level Controls) and FC (Financial Crime).

RM-2.4 Internal Audit Outsourcing

RM-2.4.1 **Licensees may not outsource their internal audit function to the same firm that acts as its external auditor.**

RM-2.4.2 **Licensees may outsource their internal audit function for a maximum period of one year, following which a licensee is expected to establish an internal audit function commensurate with the nature, scale and complexity of its business.**

RM-2.4.3 Because of the critical importance of an effective internal audit function to a licensee's control framework, all proposals to outsource internal audit operations are to be considered 'material outsourcing agreements'.

RM-2.4.4 In all circumstances, Board and management of licensees must retain responsibility for ensuring that an adequate internal audit programme is implemented, and will be held accountable in this respect by the CBB.