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	10/2019
RM-B	**Scope of Application**		
	RM-B.1	Scope	04/2005
RM-1	**General Requirements**		
	RM-1.1	Risk Management Systems and Controls	04/2014
RM-2	**Credit Risk**		
	RM-2.1	Credit Risk	01/2006
RM-3	**Liquidity Risk**		
	RM-3.1	Liquidity Risk	04/2005
RM-4	**Market Risk**		
	RM-4.1	Market Risk	04/2005
RM-5	**Insurance Technical Risk**		
	RM-5.1	Insurance Technical Risk	04/2005
RM-6	**Operational Risk**		
	RM-6.1	Operational Risk	07/2006
RM-7	**Outsourcing Risk**		
	RM-7.1	Introduction	10/2017
	RM-7.2	Supervisory Approach	10/2017
	RM-7.3	Risk Assessment	10/2017
	RM-7.4	Outsourcing Agreement	10/2017
	RM-7.5	Intra-group Outsourcing	10/2017
	RM-7.6	Internal Audit	04/2013
RM-8	**Group Risk**		
	RM-8.1	Group Risk	10/2005
RM-9	**Cyber Security Risk**		
	RM-9	Cyber Security Risk	10/2019

RM-A.1 Purpose

Executive Summary

RM-A.1.1 This Module provides detailed Rules and Guidance on risk management systems and controls requirements for insurance licensees. It expands on certain high-level requirements contained in various High-Level Standards Modules. In particular, Section AU-2.6 of Module AU (Authorisation) outlines the systems and controls required as part of the licensing conditions and Principle 10 of the Principles of Business (ref. PB-1.10) requires insurance licensees to have systems and controls sufficient to manage the level of risk inherent in their business.

RM-A.1.2 This Module obliges insurance licensees to recognise the range of risks that they face and the need to manage these effectively. Their risk management systems should monitor and control all material risks. The adequacy of a licensee's risk management is subject to the scale and complexity of its operations, however. In demonstrating compliance with certain Rules, smaller licensees with very simple operational structures and business activities may require 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) relating to risk management 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'). The Directive in this Module is applicable to insurance licensees (including their approved persons).**

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

RM-A.2.1 This Module was first issued in April 2005 by the BMA together with the rest of Volume 3 (Insurance). Any material changes that have subsequently been made to this Module are annotated with the calendar quarter date in which the change was made: UG-3 provides further details on Rulebook maintenance and version control.

RM-A.2.2 When the CBB replaced the BMA in September 2006, the provisions of this Module remained in force. Volume 3 was updated in January 2007 to reflect the switch to the CBB; however, new calendar quarter dates were only issued where the update necessitated changes to actual requirements.

RM-A.2.3 A list of recent changes made to this Module is detailed in the table below:

Module Ref.	Change Date	Description of Changes
RM-1.1	01/07/05	Correction to cross-reference
RM-6.1	01/07/05	Clarified wording of factors to consider for operational risks.
RM-2.1	01/10/05	Clarified that the 25% notification for reinsurance exposure is to be applied based on a premium basis
RM-8.1	01/10/05	Corrected cross reference to in RM-8.1.6
RM-1.1	01/01/06	Clarified CBB's requirements for insurance firms to carry out their own assessment of their capital needs.
RM-2.1	01/01/06	Corrected cross-reference.
RM-6.1	01/07/06	Added requirements for physical security measures and third party insurance to be put in place by insurance firms.
RM-A.1.3	01/2007	New Rule introduced, categorising this Module as a Directive.
RM-7.5.3	04/2008	Clarified that CBB prior approval is required for intra-group outsourcing
RM-7.2.1, 7.2.2 and 7.3.6	07/2008	Clarified that CBB prior approval is required for outsourcing arrangements
RM-7.5.7	04/2010	Added a Paragraph dealing with restrictions on intra-group outsourcing.
RM-A.1.3	01/2011	Clarified legal basis
RM-7.6	04/2013	Section amended on outsourcing of internal audit.
RM-1.1	04/2014	Enhanced the requirements for the risk management function.
RM-7.1.3	10/2017	Amended Paragraph to allow the utilization of cloud services.
RM-7.1.5A	10/2017	Added a new Paragraph on outsourcing requirements.
RM-7.2.1	10/2017	Amended Paragraph.
RM-7.2.3	10/2017	Amended Paragraph.
RM-7.2.6	10/2017	Amended Paragraph.
RM-7.2.8	10/2017	Added a new Paragraph on outsourcing.
RM-7.3.1	10/2017	Amended Paragraph.
RM-7.3.2	10/2017	Amended Paragraph.
RM-7.3.3	10/2017	Amended Paragraph.
RM-7.3.6	10/2017	Amended Paragraph.
RM-7.4.6	10/2017	Amended Paragraph.
RM-7.4.13	10/2017	Amended Paragraph.
RM-7.4.14	10/2017	Amended Paragraph.
RM-7.4.20	10/2017	Amended Paragraph.
RM-7.4.21	10/2017	Added a new Paragraph on security measures related to cloud services.
RM-7.5.3	10/2017	Amended Paragraph.
RM-7.5.4	10/2017	Amended Paragraph.
RM-9	10/2019	Added a new Section on Cyber Security.

RM-A.2.4 Guidance on the implementation and transition to Volume 3 (Insurance) is given in Module ES (Executive Summary).

RM-B.1 Scope

RM-B.1.1 **Unless otherwise stated in a Rule, or exempted in writing by the CBB, the contents of this Module apply to Bahraini insurance firms and Bahraini insurance brokers on a consolidated basis, and to overseas insurance firms and overseas insurance brokers with respect to their operations either booked in or undertaken from Bahrain.**

RM-B.1.2 Because of the nature of their activities, insurance brokers are not subject to Sections RM-4.1 (Market Risk) and RM-5.1 (Insurance Technical Risk).

RM-B.1.3 The CBB will only consider granting an exemption to a Rule in this Module, where the insurance firm concerned can demonstrate that it has equivalent systems and controls applied at the group or parent entity level, that achieve the same objective as the CBB requirement concerned. The purpose of such an exemption is to allow entity-wide or group-wide systems and requirements to be applied, where these achieve the same outcome: exemptions are therefore only likely to be given with respect to overseas insurance licensees, and possibly Bahraini licensees that are part of an overseas group. Because of their general nature, exemptions will not be considered with regards to the requirements contained in Chapter RM-1 (Risk Management Systems and Controls).

RM-B.1.4 For the purposes of Paragraph RM-B.1.1, 'consolidated basis' means including the branches and subsidiaries of the Bahraini insurance firm or Bahraini insurance broker, whether these are located inside or outside the Kingdom of Bahrain.

RM-B.1.5 **Unless otherwise stated in a Rule, or exempted in writing by the CBB, the contents of this Module apply to operators of insurance exchanges authorised to carry out insurance business in Bahrain.**

RM-B.1.6 The contents of this Module do not apply to insurance consultants, insurance managers and to appointed representatives, because the nature of their activities only expose policyholders to limited financial risk.

RM-B.1.7 While the business of insurance managers is not subject to this Module, clients of insurance managers that are insurance firms, such as captive insurers, are subject to the requirements of this Module. The insurance manager, in fulfilling its obligations to its clients, therefore needs to manage the affairs of its clients in accordance with the requirements of the Rulebook, including this Module.

RM-B.1.8 An insurance licensee's failure to establish, in the opinion of the CBB, adequate systems and controls will result in it being in breach of Condition 6 of the Licensing Conditions of Section AU-2.6 of Module AU (Authorisation). This failure may result in the CBB withdrawing or imposing restrictions on the license, or the licensee being required to inject more capital.

RM-1.1 Risk Management Systems and Controls

RM-1.1.1 **A licensee must take reasonable care to establish and maintain effective systems and controls as are appropriate to its business to manage its risks. These policies must be documented and regularly reviewed.**

RM-1.1.2 **The licensee's identification, assessment, management and reporting of risks must consider (but is not limited to) the management of credit, liquidity, market, technical, operational (including outsourcing) and group risks, as outlined in Chapters RM-2 to RM-8.**

RM-1.1.3 **As noted in Paragraph CA-A.1.2, insurance firms must regularly carry out their own assessment of their capital needs, appropriate to their risk profile, and maintain a process for monitoring and maintaining their actual capital in line with their assessment.**

RM-1.1.4 For purposes of Paragraph RM-1.1.3, the CBB does not prescribe the detailed form of such assessment, in order to give insurance firms flexibility to develop their own approaches. Where a firm's assessment suggests that a level of capital that should be held is higher than the minimum required per Chapter CA-2, the CBB would expect firms to hold capital in line with their assessment.

RM-1.1.5 **The licensee must determine if any additional risk categories, other than those referred to in Paragraphs RM-1.1.2 and RM-1.1.3, are relevant to its business and therefore need to be addressed.**

Risk Management

RM-1.1.6 **In the case of incorporated insurance firms and insurance brokers, the Board of Directors must take responsibility for the establishment and oversight of effective risk management systems and controls.**

RM-1.1.7 **In the case of Bahraini insurance brokers that are unincorporated entities or single person companies, the General Manager must take responsibility for the establishment and oversight of effective risk management systems and controls.**

RM-1.1.8 Additional requirements relating to Boards and senior management in terms of risk management and controls are specified in Module HC (High-Level Controls). The Board may delegate various functions and tasks, but retains ultimate responsibility. However, the CBB will also take into account the responsibility of the Chief Executive Officer or General Manager of a licensee, within the framework of delegated authorities laid down by the Board.

RM-1.1 Risk Management Systems and Controls (continued)

RM-1.1.9 In assessing the systems and controls framework, the CBB would expect the Board to be able to demonstrate that it provides suitable prudential oversight and establish a risk management system that includes setting and monitoring policies so that all major risks are identified, measured, monitored and controlled on an on-going basis. The risk management systems should be approved and periodically reviewed by the Board as outlined in Paragraph HC-1.1.5.

Risk Management Function

RM-1.1.10 **The CBB requires that all insurance firms establish an independent risk management function, staffed by a head of risk management, duly approved by the CBB in accordance with Paragraph AU-1.2.1.**

RM-1.1.10A **Depending on the scale and complexity of their operations, insurance brokers must consider establishing an independent risk management function.**

RM-1.1.10B **The risk management function must be independent of risk-taking units and must not have any conflict of interest with any other function. The risk management function must have direct access to the Board and must report to the Board and senior management.**

RM-1.1.11 **Where there is a risk management function, the licensee must document the process by which it manages risks, and how it directly reports to the Board of directors on these risks.**

RM-1.1.12 [This Paragraph was deleted in April 2014.]

RM-2.1 Credit Risk

RM-2.1.1 **Section RM-2.1 applies only to insurance firms and insurance brokers.**

RM-2.1.2 **Insurance licensees must identify and manage their credit risk across all their operations, and document their policies and procedures for achieving this in a credit risk policy. This policy must be regularly reviewed.**

RM-2.1.3 **Amongst other things, a licensee's credit risk policy must identify the limits it applies to both individual counterparties and categories of counterparty, how it monitors movements in counterparty risk and how it mitigates loss in the event of counterparty failure.**

RM-2.1.4 Credit risk is the risk that a counterparty will not meet its obligations in accordance with agreed terms, causing a financial loss. In the case of an insurance firm, credit risk will normally occur with:

(a) Reinsurance counterparties;
(b) Assets (e.g. stock, loans);
(c) Derivatives; and
(d) Insurance debtors (premiums due from insured persons and intermediaries).

RM-2.1.5 The licensee should consider these and other credit risk factors that may affect the licensee's solvency:

(a) The credit-worthiness of its reinsurers;
(b) The financial effect of non-performance of the reinsurance; and
(c) The financial effect of non-payment of premiums, by debtors such as intermediaries and policyholders.

RM-2.1.6 In addition to considering the failure of counterparties, the licensee should also consider scenarios such as increases in late payment and doubtful debt provisioning, and measures to mitigate credit risks, such as premium payment warranties (whereby policy coverage only becomes effective on payment of premiums).

RM-2.1.7 **An insurance firm must monitor its exposure, defined as sums insured, to an individual reinsurer and provide details of its reinsurance programme to the CBB. It must notify the CBB if its total aggregate exposure, on a premium basis, to one reinsurer (or group of related reinsurers) exceeds 25% of individual or aggregate risks and why it considers that this exposure does not pose a credit risk for which a provision should be made.**

RM-2.1 Credit Risk (continued)

RM-2.1.8 Paragraph RM-2.1.7 does not constitute a prohibition on exceeding this amount as the CBB recognises that there may be situations and types of reinsurance arrangements where reinsurance in excess of this limit might be necessary. The CBB should however be notified of these cases, and the licensee should include an explanation of the reason why it believes that the excess exposure is an acceptable credit risk.

RM-2.1.9 **In addition to the requirements noted in Paragraph RM-2.1.7, insurance firms must evaluate the credit worthiness of individual reinsurers at the time of ceding business and on an on-going basis.**

RM-2.1.10 The credit worthiness of reinsurers may be established by referring to ratings provided by international rating agencies, such as Standard & Poors or AM Best.

RM-2.1.11 **An insurance licensee must keep its exposure to individual assets or classes of assets within prudent levels, taking into account the relationship between counterparties, geographical and sectoral concentration, duration of exposures and the exposure to single loss events (e.g. regional economic downturns). Chapter CA-4 provides additional Rules in establishing limitations in the valuation of assets.**

RM-2.1.12 Specific counterparty limits are contained in Paragraph CA-4.2.33.

RM-2.1.13 **An insurance licensee must take into account the risk of default in the valuation of its assets.**

RM-3.1 Liquidity Risk

RM-3.1.1 **Section RM-3.1 applies only to insurance firms and insurance brokers.**

RM-3.1.2 **Insurance licensees must identify and manage their liquidity risk across all their operations, and document their policies and procedures for achieving this in a liquidity risk policy. This policy must be regularly reviewed.**

RM-3.1.3 Liquidity risk is the risk of not being able to meet liabilities when they fall due, even though a firm may still be solvent. Liquidity risk can result from claims falling due earlier than anticipated, higher than expected policy surrender or changes in mortality rates.

RM-3.1.4 Liquidity risk in insurance licensees relates to the management of their cash flow and the risk to their meeting short-term liabilities due to liquidity problems. The risks of matching of assets and liabilities, currency risk etc. are considered as part of insurance risk and are the subject of specific limits in Section CA-6.1.

RM-3.1.5 **Insurance licensees must also carry out stress testing to assess the resilience of their financial resources to any identified areas of material liquidity risk. This stress testing may take into account the general characteristics, and licensee's experience, of the classes of business that it writes, any discounting of its claims provisions, and any mitigating factors that it considers relevant such as the ability to sell assets quickly and the options available to re-schedule the payments to policyholders and other counterparties.**

RM-3.1.6 Where the insurance licensee considers that the nature of its assets or liabilities and the matching of its liabilities result in no significant liquidity risk exposure, it will not be expected to carry out stress testing. The CBB will expect it to document the reasons for its decision and be prepared to discuss these during an on-site visit.

RM-3.1.7 When assessing liquidity risk, the insurance licensee should consider the extent of mismatch between assets and liabilities and the amount of assets held in highly liquid, marketable forms should unexpected cash flows lead to a liquidity problem. The price concession of liquidating assets is a prime concern when assessing such liquidity risk and should be built into any assessment of capital adequacy.

RM-3.1.8 **Captive insurance firms are exempted from the specific requirement to undertake stress and scenario testing aimed at testing the resilience of their financial resources to specific areas of significant risk.**

RM-4.1 Market Risk

RM-4.1.1 **Section RM-4.1 applies only to insurance firms.**

RM-4.1.2 **Insurance licensees must identify and manage their market risk across all their operations, and document their policies and procedures for achieving this in a market risk policy. This policy must be regularly reviewed.**

RM-4.1.3 Market risk relates to the exposure of the insurance licensee, to fluctuations in the market value, currency or yield of an asset.

RM-4.1.4 **A licensee's market risk policy must identify its appetite for market risk, systems for identifying, reporting and documenting market risk and mitigation factors in place.**

RM-4.1.5 **Insurance firms (other than captives) must carry out stress testing to assess the resilience of their financial resources to any identified areas of material market risk under reasonably foreseeable circumstances. This stress testing may take into account the rating and geographical spread of its assets, the duration of their maturity relative to the licensee's liabilities and the fluctuation of interest and currency rates.**

RM-4.1.6 The insurance licensee should consider potential market risk events that may affect its solvency. These include the following:

(a) Reduced values of equities due to stock market falls, etc;
(b) Variation in interest rates and the effect on the market value of investments;
(c) A lower level of investment income than planned;
(d) Inadequate valuation of assets;
(e) The direct impact on the portfolio of currency devaluation, as well as the effect on related markets and currencies; and
(f) The extent of any mismatch of assets and liabilities.

RM-4.1.7 Chapter CA-4 contains Rules and Guidance relating to the valuation of assets and counterparty limits. Chapter CA-6 contains Rules and Guidance relating to currency matching and localisation.

RM-4.1.8 Where the insurance licensee considers that the nature of its assets and the matching of its liabilities result in no significant market risk exposure (e.g. its investments consist entirely of cash and bank deposits), it will not be expected to carry out stress testing. The CBB will expect it to document the reasons for its decision and be prepared to discuss these during an on-site visit.

RM-5.1 Insurance Technical Risk

RM-5.1.1 **Section RM-5.1 applies only to insurance firms.**

RM-5.1.2 **An insurance firm licensee must identify and manage its insurance technical risk across all its operations, and document its underwriting and claims policies for achieving this in an underwriting policy.**

RM-5.1.3 Insurance technical risk is the normal trading risk, arising out of contracts of insurance, that the insurance licensee is exposed to in its day-to-day operations, and includes the technical and actuarial bases of calculation for premiums and technical provisions in both long-term and general insurance.

RM-5.1.4 **An insurance firm must document its underwriting and claims policies and review these at regular intervals.**

RM-5.1.5 **The underwriting policy must be at a level of detail appropriate to the nature, magnitude and source of its business and must include (but is not limited to) a description of the following elements:**

(a) Classes and sources of business to be written (including limits on concentrations of class, location and counterparty);
(b) Rating and pricing strategy and methodology;
(c) The management of, and reserving for, claims;
(d) Responsibilities and authority levels; and
(e) Reinsurance protections, including any mismatch between the duration of the contracts and the underlying reinsurance protection.

RM-5.1.6 **The claims policy must be at a level of detail appropriate to the nature, magnitude and source of its business and must include (but is not limited to) a description of the following elements:**

(a) Reporting (e.g. evidence required, appointment of loss adjusters);
(b) Scrutiny;
(c) Authority levels;
(d) Valuation;
(e) Monitoring claims settlement, payments, reinsurance recoveries and subrogation; and
(f) Provisioning of claims, including the bases and assumptions followed, authority levels, record-keeping and review.

RM-5.1 Insurance Technical Risk (continued)

RM-5.1.7 **Where necessary to demonstrate the adequacy of its financial resources under reasonably foreseeable deteriorations of its underwriting and claims positions, the insurance firm must conduct stress testing under a range of foreseeable adverse scenarios.**

RM-5.1.8 **In assessing the outcome of adverse scenarios on the future solvency position, insurance firms must consider the impact of future further deterioration claims reserves (or, in the case of long-term business, the inadequacy of mathematical reserves) and future loss ratios being higher than past claims patterns would suggest.**

RM-5.1.9 Factors that licensees may consider appropriate in assessing the levels of underwriting risk include:

(a) The adequacy of the licensee's pricing structure;
(b) The volatility of sales volumes (e.g. the risk of poor underwriting from over-rapid expansion);
(c) The uncertainty of claims experience (and the length of the claims 'tail');
(d) The share of premium paid to intermediaries;
(e) The adequacy of the coverage of the reinsurance programme;
(f) The impact of the licensee's inability to secure renewal of part of its reinsurance at acceptable terms or at all;
(g) The risk of unintended risks claims being covered (or not excluded) by policy wordings; and
(h) The risk of mis-selling, for example, the number of complaints or disputed claims.

RM-5.1.10 Factors that insurance licensees may consider appropriate in assessing the levels of claims risk include:

(a) The frequency and size of large claims;
(b) Possible outcomes relating to any disputed claims, particularly where the outcome is subject to legal proceedings;
(c) The ability of the licensee to withstand catastrophic events, increases in unexpected exposures, latent claims or aggregation of claims;
(d) The possible exhaustion of reinsurance arrangements, both on a per-risk and per-event basis;
(e) The non-payment of outstanding claims due to the lack of coverage offered by the reinsurance purchased for underwritten risks (i.e. offsetting potential liabilities);
(f) Social changes regarding an increase in the propensity to claim and to sue;
(g) The impact of unanticipated legal judgements on claims and claims reserves;
(h) Other social, economic and technological changes; and
(i) The risk associated with dealing with a reinsurer, fronting 100% of the risks ceded.

RM-5.1 Insurance Technical Risk (continued)

RM-5.1.11 The CBB believes that insurance firms need to consider carefully dealing with reinsurers fronting 100% of the risks that is ceded to them. The concern is that the reinsurer ceding 100% of the risk to a retrocessionaire has little incentive to adhere to proper standards of underwriting, due to it receiving a fee, based on maximizing volume of premium, at the expense of underwriting soundness. Fronting arrangements can result in abrupt cancellation by the assuming reinsurer and sometimes refusal to pay claims because of the lack of observation of the understandings with regard to business quality that were agreed upon when the arrangement was negotiated. Consequently, insurers may have to assume risks for which they believed to have covered through a proper reinsurance arrangement, should the reinsurer no longer honour the arrangement. The CBB will scrutinise carefully the management by firms of the risks associated with fronting, in the course of its supervision.

RM-5.1.12 Additional factors that general insurers may consider appropriate in assessing the levels of claims risk include:

(a) The adequacy and uncertainty of the technical claims provisions, such as outstanding claims, IBNR and claims handling expense reserves;
(b) The adequacy of other underwriting provisions, such as the provisions for unearned premium and unexpired risk reserves;
(c) The appropriateness of catastrophe models and underlying assumptions used, such as possible maximum loss (PML) factors used; and
(d) The effects of inflation.

RM-5.1.13 Additional factors that long-term insurers may consider appropriate in assessing the levels of claims risk include future variations in investment returns and in mortality and morbidity rates.

RM-6.1 Operational Risk

RM-6.1.1 **Section RM-6.1 applies only to insurance firms and insurance brokers**

RM-6.1.2 **An insurance licensee must identify and manage its operational risk across all its operations, and document its policies and procedures for achieving this in an operational risk policy.**

RM-6.1.3 Operational risk is the risk to the insurance licensee of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

RM-6.1.4 **Insurance licensees must consider the impact of operational risks on their financial resources and solvency. In so doing, insurance licensees must consider the factors listed under Paragraph RM-6.1.5, and any other factors relevant to their business.**

RM-6.1.5 In assessing potential operational risk, events that may affect the licensee's solvency include the following:

(a) Risks to the licensee's resources and reputation from employees and agents (due to fraud, negligence etc);
(b) Adequacy of management information;
(c) Failure of information technology through breakdown, incompatibility of legacy systems and poor scalability, poor security, etc.;
(d) Failure of processes and procedures;
(e) Internal and external fraud;
(f) Outsourcing risk (for more detail, see RM-7);
(g) Resourcing levels;
(h) Business continuity and disaster recovery; and
(i) Reputational risks and the risk to the licensee's business from an undermining of consumer confidence in particular market segments, e.g. savings products.

RM-6.1.6 Human failure may arise either from the loss of one or more key individuals, lack of competence or failure of an individual to follow procedures or observe authority levels.

RM-6.1 Operational Risk (continued)

RM-6.1.7 **The insurance licensee must identify those processes, systems and premises that are critical to its survival and continuing operations and must develop contingency plans ('business continuity planning') covering these areas. These plans must be regularly updated and tested.**

RM-6.1.8 An insurance licensee should have the means to ensure that its statutory and regulatory responsibilities are effectively carried out, especially where the group is subject to matrix management. More specifically, clear reporting lines and responsibilities need to be defined to minimize the risk that statutory and regulatory responsibilities are overlooked.

RM-6.1.9 **Insurance licensees must ensure that there is adequate succession planning and that the risks arising from the loss of key individuals are thereby contained.**

RM-6.1.10 **The licensee's Board is responsible for ensuring the suitability and competence of employees for the assigned tasks, and for the adequacy of staffing levels. Depending on their size and scale of their activities, insurance licensees should consider having in place a formal appraisal process and a training plan for professional members of staff. For employees that are members of professional bodies it may also be appropriate for this to be integrated with requirements of those bodies for Continuing Professional Education (CPE).**

RM-6.1.11 **Insurance licensees must identify, manage and control the risks that arise from human failure, including employees and agents. These include inappropriate remuneration policies, health and safety and employment policies.**

RM-6.1.12 **The licensee's business continuity planning, risk identification and reporting must cover reasonably foreseeable external events and their likely impact on the firm and its business portfolio.**

Physical Security Measures

RM-6.1.13 **Insurance licensees that deal directly with the public and maintain cash on their premises must put in place security measures to minimise the risk of theft or fraud.**

RM-6.1 Operational Risk (continued)

RM-6.1.14 **Insurance licensees subject to Paragraph RM-6.1.13 must ensure that the maximum cash maintained at their premises at the end of each day is limited to BD10,000.**

RM-6.1.15 **Insurance licensees subject to Paragraph RM-6.1.13 are required to install an alarm system for those premises that maintain cash.**

RM-6.1.16 Where appropriate, insurance licensees may consider the need to maintain a trained security guard at their premises.

Third Party Insurance

RM-6.1.17 **Insurance licensees are required to have in place insurance coverage from an unrelated third party to cover potential losses arising from liability, theft, fire and other potential operational risk.**

RM-6.1.18 Insurance licensees are required to comply with Paragraph RM-6.1.13 to 6.1.17, by 31st December 2006 (Refer to ES-2.6A.1).

RM-7.1 Introduction

RM-7.1.1 **Section RM-7.1 applies only to insurance firms and insurance brokers.**

RM-7.1.2 **An insurance licensee must identify all material outsourcing contracts and ensure that the risks associated with such contracts are adequately controlled. In particular, insurance licensees must comply with the specific requirements set out in this Chapter.**

RM-7.1.3 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-7.1.4 It is recognised that benefits can potentially be achieved through outsourcing an activity to a third party provider. They include reduced costs, enhanced service quality and a reduction in management time spent on non-core activities. However, outsourcing an activity also poses potential risks. These include the suitability or otherwise of the service provider, business continuity, reduced control over the activity and access to relevant information, and increased legal and client confidentiality risks.

RM-7.1.5 For purposes of Paragraph RM-7.1.2, 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-7.1.5A 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-7.1.6 An outsourcing agreement between a CBB licensed insurance manager and captive insurer is not considered material for the purposes of RM-7, because the provider is another regulated entity. Nonetheless, Boards of these insurance managers should consider the Rules and Guidance in this Chapter to be relevant to them as Guidance and should consider applying these as good practice.

RM-7.1.7 **Insurance 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-7.2 Supervisory Approach

RM-7.2.1 **A licensee must seek the CBB's prior written approval before committing to a new material outsourcing arrangement.**

RM-7.2.2 **The prior approval request must:**

(a) Be made in writing to the licensee's normal supervisory contact;

(b) Contain sufficient detail to demonstrate that relevant issues raised in Section 3 onwards of this Chapter have been addressed; and

(c) Be made at least 6 weeks before the licensee intends to commit to the arrangement.

RM-7.2.3 The CBB will review the information provided and provide a definitive response within 6 weeks of receiving the request for approval. Where further information is requested from the licensee, however, the time taken to provide this further information will not be taken into account. The CBB may also contact home supervisors or host supervisors to seek their comments – in such cases, the 6-week turnaround is also subject to the speed of their response.

RM-7.2.4 **Once an activity has been outsourced, a licensee must continue to monitor the associated risks and the effectiveness of its mitigating controls.**

RM-7.2.5 **A licensee must immediately inform its normal supervisory contact at the CBB of any material problems encountered with the outsourcing provider.**

RM-7.2.6 **The CBB may direct a licensee to make alternative arrangements for the outsourced activity.**

RM-7.2.7 **The CBB will also require on-going access to the outsourced activity, which it may occasionally want to examine itself, through management meetings or on-site examinations.**

RM-7.2.8 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-7.3 Risk Assessment

RM-7.3.1 **Licensees must undertake a thorough risk assessment of an outsourcing proposal, before formally submitting the request for approval to the CBB and committing itself to an agreement.**

RM-7.3.2 The risk assessment should – amongst other things – include an analysis of (i) the business case; (ii) the suitability of the outsourcing provider including but not limited to the outsourcing provider's financial soundness, its technical competence, its commitment to the arrangement, its reputation, its adherence to international standards, and the associated country risk; and (iii) the impact of the outsourcing on the licensee's overall risk profile and its systems and controls framework.

RM-7.3.3 In assessing the suitability of the outsourcing provider, the licensee should also consider the adequacy of its human resources, the capacity, scalability and resilience of systems and processes and arrangements for the transfer or insourcing of the services either at the end of the contract or sooner should the need arise. The firm's Board is also responsible for ensuring that adequate arrangements and information are available for monitoring the performance of the outsourced services.

RM-7.3.4 Before entering into an outsourcing agreement, the CBB expects licensees to have undertaken a thorough assessment of a proposal before formally submitting a notification to the CBB. However, the CBB is also willing to discuss ideas informally at an early stage of development, on a 'no-commitment' basis. It especially encourages an early approach when the proposed outsourcing is particularly material or innovative.

RM-7.3.5 **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-7.3.6 **A licensee must nominate a relevant approved person with day-to-day responsibility for handling the relationship with the outsourcing provider and ensuring that relevant risks are addressed. The CBB should be informed of the designated individual as part of the written prior approval required under Section RM-7.2 above. Any subsequent replacement of such person must also be notified to the CBB.**

RM-7.4 Outsourcing Agreement

RM-7.4.1 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-7.4.2 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-7.4.3 Any material outsourcing arrangement by a licensee must be the subject of a legally enforceable contract. Where the outsourcing provider interacts directly with a licensee's customers, the contract should – where relevant – reflect the licensee's own standards regarding customer care.

RM-7.4.4 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. Mechanisms for the regular monitoring by licensees of performance against Service Level Agreement and other targets, and for implementing remedies in case of any shortfalls, must also form part of the agreement. Such reviews should take place at least every year.

RM-7.4.5 Clear reporting and escalation mechanisms must be specified in the agreement.

RM-7.4.6 Where an outsourcing provider in turn decides to sub-contract to other providers, CBB's prior written approval must be obtained, and the original provider must remain contractually liable to the licensee for the quality and level of service agreed, and its obligations to the licensee must remain unchanged.

RM-7.4 Outsourcing Agreement (continued)

Customer Data Confidentiality

RM-7.4.7 **Licensees must ensure that outsourcing agreements comply with all applicable legal requirements regarding customer confidentiality.**

RM-7.4.8 **Licensees must ensure that the outsourcing provider implements adequate safeguards and procedures.**

RM-7.4.9 For purposes of Paragraph RM-7.4.8, the implementation of adequate safeguards and procedures would include the proper segregation of customer data from those belonging to other clients 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 a breach of confidentiality.

RM-7.4.10 **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 firm.**

RM-7.4.11 **Licensees must assess the impact of using an overseas-based outsourcing provider on their ability to maintain customer data confidential, for instance, because of the powers of local authorities to access such data.**

Access to Information

RM-7.4.12 **Outsourcing agreements must ensure that the licensee's 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-7.4.13 **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 law. Such access must allow the CBB to conduct on-site examinations of the outsourcing provider, if required.**

RM-7.4 Outsourcing Agreement (Continued)

RM-7.4.14 Where the outsourcing provider is based overseas, the outsourcing provider must confirm in the outsourcing agreement that there are no regulatory or legal impediments to either the licensee's internal and external auditors, or the CBB inspectors and appointed experts, having the access described in Paragraphs RM-7.4.12 and RM-7.4.13 above. Should such restrictions subsequently be imposed, the licensee must communicate this fact to the CBB as soon as it becomes aware of the matter.

RM-7.4.15 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-7.4.16 Licensees must ensure that service providers maintain, regularly review and test plans to ensure continuity in the provision of the outsourced service.

RM-7.4.17 Licensees must have an adequate understanding of the outsourcing provider's arrangements, to understand the implications for its own contingency arrangements as per Paragraph RM-7.3.5.

Termination

RM-7.4.18 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-7.4.19 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-7.4 Outsourcing Agreement (Continued)

RM-7.4.20 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-7.4.21 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-7.5 Intra-group Outsourcing

RM-7.5.1 **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-7.5.2 However, the degree of formality required – in terms of contractual agreements and control mechanisms - for outsourcing within a licensee's group is likely to be less, because of common management and enhanced knowledge of other group companies.

RM-7.5.3 **A licensee must obtain CBB prior written approval before committing to a material intra-group 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.**

RM-7.5.4 The CBB will respond to the request for approval in the same manner and timescale as set out in Section RM-7.2 above.

RM-7.5.5 The CBB expects, as a minimum, an agreed statement of the standard of service to be provided by the group provider, including a clear statement of responsibilities allocated between the group provider and licensee.

RM-7.5.6 The CBB also expects a licensee's management to have addressed the issues of customer confidentiality, access to information and business continuity covered in Section RM-7.4 above.

RM-7.5.7 **Insurance licensees may not outsource their core business activities 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-7.6 Internal Audit

RM-7.6.1 Because of the critical importance of an effective internal audit function to a licensee's control framework (as outlined in Section HC-3.3), all proposals to outsource internal audit operations are to be considered 'material outsourcing agreements' for the purposes of Paragraph RM-7.2.1.

RM-7.6.2 **Licensees may not outsource their internal audit function to the same firm that acts as their external auditor.**

RM-7.6.3 [This Paragraph was deleted in April 2013].

RM-7.6.4 **All requests to outsource the internal audit function must be supported by a board resolution or ratified by the audit committee.**

RM-7.6.5 **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.**

RM-8.1 Group Risk

RM-8.1.1 **Section RM-8.1 applies only to Bahraini insurance firms and Bahraini insurance brokers.**

RM-8.1.2 An insurance licensee must identify, manage and control risks to its activities arising from the activities and financial position of other members of its group.

RM-8.1.3 The CBB may impose additional restrictions on the insurance licensee should it have reason to believe that other members of the group pose undue risk to the insurance licensee. These restrictions, for instance, may try to limit the risk of financial contagion, by restricting financial transactions between the licensee and group members.

RM-8.1.4 For purposes of Section RM-8.1, the term group refers to a person or firm who is:
(a) The parent of the licensee;
(b) A subsidiary of the licensee (including subsidiaries of subsidiaries); or
(c) A subsidiary of the licensee's parent.

RM-8.1.5 **The Board is expected to request sufficient information of its group members to allow it to address group risks.**

RM-8.1.6 **Where the licensee's group or parent reports its own solvency position to its regulatory authority (on a group or 'solo' basis), a copy of this calculation must be provided to the CBB within 30 calendar days from the due date to the other regulatory authority, in accordance with Paragraph CA-7.1.8.**

RM-8.1.7 Where a licensee is part of a larger financial services group, it may rely on the systems and controls that the group (or its parent company) has put in place. The Board in these circumstances should establish what systems and controls are in place and should ensure that it is provided with sufficient and timely information on the solvency position of the group. This should be evidenced in the prudential records retained in Bahrain.

RM-8.1 Group Risk (continued)

RM-8.1.8 **In assessing group systems and controls, an insurance licensee must give consideration to:**

(a) The likely impact of activities of the group on the compliance of the licensee with CBB requirements;

(b) The effectiveness of linkages between group central functions and the licensee;

(c) Potential conflicts of interest and methods of minimising them; and

(d) The risk of adverse events of other group entities on the licensee, in particular due to financial weakness, crime or fraudulent behaviour.

RM-8.1.9 An insurance licensee should not be subject to material influence by other entities of the group through informal or undocumented channels. The overall governance, high-level controls and reporting lines with the group should be clearly documented.

RM-9.1 Cyber Security Risk Measures

RM-9.1.1 Insurance licensees must establish clear ownership and management accountability for the risks associated with cyber-attacks. They must establish the related risk management processes commensurate with their size, nature of activities and risk profiles. Cyber security measures must be made part of the licensee's IT security policy.

Training

RM-9.1.2 The licensees must ensure that all employees receive adequate training on a regular basis, in relation to cyber security and the threats they could encounter, such as through testing employee reactions to simulated cyber-attack scenarios. All relevant employees must be informed on the current cyber security breaches and threats.

Role of Board and Senior Management

RM-9.1.3 The Board and senior management of the licensees must ensure that effective risk management practices are in place to address cyber security risks and that cyber security controls are periodically evaluated taking into account industry best practices and emerging cyber threats.

RM-9.1.4 The Board of the insurance licensee must be responsible for:

a) Setting and approving a cyber risk strategy commensurate with the size, nature of activities and the risk profile;
b) Ensuring that cyber roles within the organization have been aligned to the cyber risk strategy;
c) Approving a cyber risk management framework;
d) Determining the manner in which it oversees implementation of the cyber risk management framework by senior management; and
e) Receiving reports on all cyber incidents.

RM-9.1 Cyber Security Risk Measures (continued)

RM-9.1.5 The senior management of an insurance licensee must be responsible for the following activities:

(a) Creating an overall cyber risk management framework commensurate with the size, nature of activities and the risk profile of the licensee and formulating a cyber risk defense policy;

(b) Regularly measures the effectiveness of the implementation of the risk management practices mentioned in RM-9.1.3 and ensuring that this is regularly reported to the Board;

(c) Ensuring that process for identifying critical internal functions are in place and annually verified;

(d) Adequately overseeing the implementation of the cyber risk management framework;

(e) Implementing and consistently maintaining an integrated, corporate-wide, cyber risk management framework, including sufficient resource allocation;

(f) Monitoring the effectiveness of the cyber defense array and coordinating cyber defense activities with internal and external risk management entities;

(g) Receiving periodic reports from the relevant departments on the current situation with respect to cyber threats and cyber risk treatment; and

(h) Receiving periodic reports on all cyber incidents (internal and external) and analysis of their implications on the licensee.

RM-9.1.6 Cyber security risk must be an item for discussion at Board meetings.

RM-9.1.7 The Board must ensure that the cyber security risk policy and procedures are robust and can comprehensively assist the licensee's cyber security requirements. In the case of branches, it is recommended that there is a formal sign-off of a localised version of such policy.

RM-9.1.8 A clear reporting line to the Board must be established for cyber security risk incidents. A dedicated IT Security Officer must be appointed with responsibility for cyber and information security.

RM-9.1 Cyber Security Risk Measures (continued)

RM-9.1.9 A corporate-wide cyber security risk defense strategy must be defined and documented, which includes:

a) The position and importance of cyber security risk defense at the licensee;
b) The cyber security risk-threat concept and the challenges facing the licensee;
c) The licensee's approach to cyber security risk management, definition and oversight of the level of exposure to cyber security risk threats; and
d) The key elements of cyber security risk defense strategy – objectives, principles of operation and implementation.

RM-9.1.10 Licensees must establish a cyber security risk policy, which includes:

a) Cyber defense objectives, definition of areas of responsibilities, involved positions and functions (including work interfaces);
b) Organisational structures, structure and governance of the cyber security risk management process at the licensee;
c) Internal procedural framework of the licensee, details of the controls required and the framework for their implementation;
d) Monitoring and responses, training and awareness, information gathering, research, and sharing;
e) Process maturity and effectiveness metrics and indices; and
f) Evaluation, control and reporting.

RM-9.1.11 Licensees must conduct a periodic assessment of cyber defense controls. Cyber defense control assessment must include an analysis of the controls' current status vis-à-vis relevant cyber security risk threats, weaknesses and risks across the different activity segments, including:

a) Physical access, administration and organization;
b) Information system life-cycle in various operational environments;
c) Technology management and critical supporting systems;
d) Interaction with customers, devices used by customers;
e) Remote access, messaging and communication;
f) Identity and access management, business partners and suppliers, information and data exchange channels; and
g) Organisational culture and awareness, online presence, online activities and use of social networks, and business continuity.

RM-9.1 Cyber Security Risk Measures (continued)

RM-9.1.12 Licensees must arrange to seek cyber security risk insurance cover from an independent insurer once the assessment of cyber security risk is complete. The insurance policy may include some or all of the following types of coverage, depending on the risk assessment outcomes;

a) Crisis management expenses such as costs of notifying affected parties, costs of forensic investigation, costs incurred to determine the existence or cause of a breach, regulatory compliance costs, costs to analyse the insured's legal response obligations;

b) Claim expenses such as costs of defending lawsuits, judgments and settlements, and costs of responding to regulatory investigations;

c) Policy must also provide coverage for a variety of torts, including invasion of privacy or copyright infringement. First-party coverages may include lost revenue due to interruption of data systems resulting from a cyber or denial of service attack and other costs associated with the loss of data collected by the insured.

Security Breach

RM-9.1.13 Licensees must have suitable processes in place to verify the validity of all requests received through all methods of communication including email such as a phish alert solution. Licensees must also ensure that mobile devices with access to their systems, applications and networks are protected through security measures such as mobile device management, encryption, remote wipe, and password protection.

RM-9.1.14 Licensees must report to the CBB any instances of cyber-attacks immediately, whether internal or external, that compromise customer information or disrupt critical services that affect their operations. In addition, licensees must provide the root cause analysis of the cyber-attack and measures taken by them to ensure that similar events do not recur, within 5 working days. Any significant attack or breach to the system regardless of whether it caused loss or damage, must be reported to the CBB.

RM-9.1 Cyber Security Risk Measures (continued)

Independent testing

RM-9.1.15 All licensees providing internet services must test their systems against security breaches and verify the robustness of the security controls in place each year in June and December. These tests must be conducted by security professionals, such as ethical hackers, that provide penetration testing services and a vulnerability assessment of the system. The tests must be undertaken by external independent consultants.

RM-9.1.16 The vulnerability assessment report referred to in paragraph RM-9.1.15 must be provided to the CBB within two months following the end of the month where the testing took place, i.e. for the June test, the report must be submitted at the latest by 31st August and for the December test, by 28th February.