RISK MANAGEMENT MODULE

MODULE:	RM (Risk Management)

Table of Contents

RM-A.1 Purpose

Executive Summary

RM-A.1.1 This Module contains requirements relating to the management of risk by investment firm licensees. 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 investment firm licensees 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 investment firm 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.

RM-A.1.3 The requirements contained in this Module apply to Category 1 investment firms and Category 2 investment firms only.

Legal Basis

RM-A.1.4 **This Module contains the Central Bank of Bahrain's ('CBB') Directive (as amended from time to time) regarding Risk Management requirements applicable to investment firm 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').**

RM-A.1.5 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 July 2007, as part of the second phase release of Volume 4's contents. It is dated July 2007. All subsequent changes to this Module are annotated with the end-calendar quarter date in which the change was made: 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-1.1.11	04/2008	Clarified the requirement for investment firm licensees to have a separate risk management function.
RM-7.3.3	04/2008	Clarified that CBB prior approval is required for intra-group outsourcing.
RM-7.1.6, 7.1.7 and 7.1.16	07/2008	Clarified that CBB prior approval is required for outsourcing arrangements.
RM-B.1.2	10/2009	Amended to reflect applicability of Chapters RM-7 and RM-8.
RM-7.1.16	10/2009	Amended to read approved person.
RM-7.3.7	10/2009	New Rule added to clarify that licensees may not outsource core business activities, including internal audit, to their group.
RM-7.4	10/2009	Updated to reflect CBB's requirements for outsourcing the internal audit function.
RM-1.1.10, RM-1.1.11, and RM-1.1.13	07/2010	Updated and amended to include requirements for the risk management function.
RM-7.1.7	07/2010	New Rule added regarding outsourcing core business functions or activities to third parties.
RM-A.1.4	01/2011	Clarified legal basis.
RM-B.2	01/2011	Removed reference in title to affiliates.
RM-4.1.8 and RM-4.1.9	07/2012	Replaced reference to "securities" with "financial instruments".
RM-7.4.5	10/2012	Corrected typo.
RM-7.4.2A	01/2013	New Paragraph added to require that the outsourcing of the internal audit function must be supported by a board resolution or ratified by the audit committee.
RM-7.1.9	07/2013	Added cross reference.
RM-7.1.9A and RM-7.3.4	07/2013	Made reference to considerable outsourcing.
RM-7.4.4	07/2013	Changed Guidance to Rule.
RM-1.1.10 to RM-1.1.14	10/2013	Amendments made to allow overseas investment firm licensees to outsource the risk management function to their head office, subject to the CBB's prior written approval.
RM-1.1.7	01/2016	Corrected cross reference.
RM-1.1.9	01/2016	Aligned risk categories as per Module RM.
RM-4.1.17	01/2016	Restructured Subparagraphs to avoid duplication.
RM-7.1.9	01/2016	Clarified Guidance.
RM-7.1.1	10/2017	Amended Paragraph to allow the utilization of cloud services.
RM-7.1.3A	10/2017	Added a new Paragraph on outsourcing requirements.
RM-7.1.6	10/2017	Amended Paragraph.
RM-7.1.9	10/2017	Amended Paragraph.
RM-7.1.11	10/2017	Amended Paragraph.
RM-7.1.11A	10/2017	Added a new Paragraph on outsourcing.
RM-7.1.13	10/2017	Amended Paragraph.
RM-7.1.14	10/2017	Amended Paragraph.
RM-7.1.14(f)	10/2017	Added a new sub-Paragraph.

RM-A.2 Module History (continued)

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

Module Ref.	Change Date	Description of Changes
RM-7.1.17	10/2017	Amended Paragraph.
RM-7.2.4	10/2017	Amended Paragraph.
RM-7.2.11	10/2017	Amended Paragraph.
RM-7.2.12	10/2017	Amended Paragraph.
RM-7.2.18	10/2017	Amended Paragraph.
RM-7.2.19	10/2017	Added a new Paragraph on security measures related to cloud services.
RM-7.3.3	10/2017	Amended Paragraph.
RM-7.3.4	10/2017	Amended Paragraph.
RM-9.1	04/2019	Added a new Chapter on Cyber Security Risk .

Superseded Requirements

RM-A.2.3 This Module does not replace any regulations or circulars in force prior to July 2007.

RM-A.2.4 Further guidance on the implementation and transition to Volume 4 (Investment Business) is given in Module ES (Executive Summary).

RM-B.1 License Categories

RM-B.1.1 **The contents of this Module – unless otherwise stated – apply to Category 1 and Category 2 investment firms only.**

RM-B.1.2 **Category 3 investment firms – unless otherwise stated – are exempted from the requirements of this Module with the exeption of Chapters RM-7 and RM-8.**

RM-B.1.3 In respect of Category 3 investment firms, however, the specific requirements contained in Module RM should be considered as good practice, which it may be appropriate to apply. Notwithstanding the exemption from the specific requirements of Module RM, specified in Rule RM-B.1.2, Category 3 investment firms are nonetheless required to maintain adequate systems and controls (see Sections AU-2.6 and PB-1.10).

RM-B.2 Branches and Subsidiaries

Bahraini Investment Firm Licensees

RM-B.2.1 **Bahraini investment firm licensees must ensure that, as a minimum, the same or equivalent provisions of this Module apply to their branches, whether located inside or outside the Kingdom of Bahrain, such that these are also subject to an effective risk management framework. In instances where local jurisdictional requirements are more stringent than those applicable in this Module, the local requirements are to be applied.**

RM-B.2.2 **Bahraini investment firm licensees must satisfy the CBB that their subsidiaries and other group members (where relevant) are subject to appropriate arrangements such that they too effectively manage their risks.**

RM-B.2.3 Where an investment firm licensee is unable to satisfy the CBB that its subsidiaries and other group members are subject to appropriate risk management arrangements, the CBB will assess the potential impact of risks – both financial and reputational – that this poses to the investment firm licensee. The CBB recognises that different types of activity require different approaches to risk management, and it does not necessarily expect arrangements to be in place elsewhere in a group equivalent to those contained in this Module. However, where the CBB assesses that risk management weaknesses in subsidiaries and other group members pose material risks to the investment firm licensee, the CBB may impose restrictions on dealings between the licensee and other group members. Where such weaknesses are assessed by the CBB to pose a major threat to the stability of the investment firm licensee, then its authorisation may be called into question.

Overseas Investment Firm Licensees

RM-B.2.4 **Overseas investment firm licensees must satisfy the CBB that the same or equivalent arrangements to those contained in this Module are in place at the head office level, as well as ensuring that there is effective risk management of activities conducted under the Bahrain license.**

RM-B.2.5 In assessing compliance with Paragraph RM-B.2.4, the CBB will take into account regulatory requirements applicable to the head office, i.e. the company of which the Bahrain branch is part, as well as the risk management framework applied to the Bahrain operation. With the exception of specific requirements that explicitly apply to overseas investment firm licensees, overseas investment firm licensees should consider the contents of this Chapter as guidance, in judging whether risk management controls applied to the branch satisfy RM-B.2.4.

RM-1.1 Risk Management

Board of Directors' Responsibility

RM-1.1.1 **The Board of Directors of investment firm 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 investment firm licensee 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 An investment firm licensee'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 investment firm 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-1.2.10.

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

RM-1.1 Risk Management (continued)

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, including the major sources of risk in each of the following Categories:

(a) Counterparty risk;
(b) Market risk;
(c) Liquidity risk;
(d) Operational risk;
(e) Derivative Transactions Risk;
(f) Outsourcing Risk;
(g) Group Risk; and
(h) Any additional categories relevant to its business.

Risk Management Function

RM-1.1.10 **A Bahraini investment firm licensee must have a risk management function commensurate with the nature, scale and complexity of its business.**

RM-1.1.11 **Where a licensee maintains a risk management function, this function must be independent of risk-taking units. The duties of the risk management function include but are not limited to:**

(a) Identifying, measuring, monitoring, and controlling the major sources of risks associated with the operations of the Bahraini investment firm licensee including any entity it may own, control or manage on an ongoing basis;

(b) Reporting to the Board and senior management on all material risks to the licensee; and

(c) Documenting the processes and systems by which it identifies and monitors material risks, and how it reports to the Board and senior management these risks.

RM-1.1.12 The CBB will only consider a licensee not having a risk management function, where its investment activities are limited in scale and complexity, and appropriate mitigating controls are in place.

RM-1.1.13 **Unless otherwise agreed in writing with the CBB, the risk management function of a Bahraini investment firm licensee, may not be outsourced to a third party.**

RM-1.1 Risk Management (continued)

RM-1.1.14 An overseas investment firm licensee may establish a risk management function commensurate with the nature, scale and complexity of its business. The risk management function may be combined with another function. The CBB will consider an overseas investment firm licensee not having a local risk management function, provided that it seeks CBB's approval to outsource this function to its Head Office, in accordance with Section RM-7.3 (Intra-group Outsourcing). In such case, the CBB must be satisfied that equivalent arrangements to those contained in this Module are in place at the Head Office level, and that such arrangements would entail effective risk management of activities conducted by the overseas investment firm licensee.

RM-2.1 Counterparty Risk

RM-2.1.1 **Investment firm licensees must document in a credit policy their 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-2.1.2 **Among other things, the 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-2.1.3 A licensee's credit risk policy should provide a clear indication of the amount and nature of counterparty risk that the licensee wishes to incur. In particular, it should cover:

(a) How, with particular reference to its activities, the licensee defines and measures credit risk;

(b) The types and sources of counterparty risk to which the licensee wishes to be exposed (and the limits on that exposure) and those to which the investment firm licensee wishes not to be exposed (and how that is to be achieved, for example how exposure is to be avoided or mitigated); and

(c) The level of diversification required by the licensee and the licensee's tolerance for risk concentrations (and the limits on those exposures and concentrations).

RM-2.1.4 It is important that sound and legally enforceable documentation is in place for each agreement that gives rise to counterparty risk as this may be called upon in the event of a default or dispute. A licensee should therefore consider whether it is appropriate for an independent legal opinion to be sought on documentation used by the licensee. Best practise would dictate that documentation should normally be in place before the licensee enters into a contractual obligation or releases funds.

Risk Monitoring

RM-2.1.5 **Investment firm licensees must implement an effective system for monitoring counterparty risk which should be described in a credit risk policy.**

RM-2.1.6 **Investment firm licensees must meet the Counterparty Risk Requirements in Module CA-3.3. The licensee must monitor its exposures and must notify the CBB if its total exposure to an individual counterparty exceeds 25% of aggregate counterparty exposures and/or 25% of the licensee's regulatory capital.**

RM-2.1 Counterparty Risk (continued)

RM-2.1.7 Individual credit facilities and overall limits should be periodically reviewed, in order to check their appropriateness for both the current circumstances of the counterparty and the firm's current internal and external economic environment. The frequency of review should be appropriate to the nature of the facility, but in any event should take place at least once a year.

Record Keeping

RM-2.1.8 **Investment firm licensees must maintain appropriate records of:**

(a) Counterparty exposures, including aggregations of individual counterparty exposures, as appropriate, by:
- **(i) Groups of connected counterparties;**
- **(ii) Types of counterparty as defined, for example, by the nature or geographical location of the counterparty;**

(b) Investment decisions, including details of the decision and the facts or circumstances upon which it was made; and

(c) Information relevant to assessing current counterparty and risk quality.

RM-2.1.9 For the purposes of this Module, connected counterparties means all undertakings with which the licensee has close links; the Directors (and their family) of the licensee; and the Directors (and their family) of undertakings with which the licensee has close links.

RM-3.1 Liquidity Risk

RM-3.1.1 **Investment firm licensees must maintain a liquidity risk policy for the management of liquidity risk of the licensee, 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-3.1.2 **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-3.1.3 The liquidity risk policy should cover the general approach that the licensee will take to liquidity risk management, including, as appropriate, various quantitative and qualitative targets. This general approach should be communicated to all relevant functions within the organisation.

RM-3.1.4 The policy for managing liquidity risk should cover specific aspects of liquidity risk management. So far as appropriate to the nature, scale and complexity of the activities carried on, such aspects might include:

(a) The basis for managing liquidity (for example, regional or central);
(b) The degree of concentrations, potentially affecting liquidity risk, that are acceptable to the firm;
(c) A policy for managing the liability side of liquidity risk;
(d) The role of marketable, or otherwise realisable, assets;
(e) Ways of managing both the licensee's aggregate foreign currency liquidity needs and its needs in each individual currency;
(f) Ways of managing market access;
(g) The use of derivatives to minimise liquidity risk;
(h) The management of intra-day liquidity, where this is appropriate, for instance where the licensee is a member of or participates (directly or indirectly) in a system for the intra-day settlement of payments or transactions in investments; and
(i) Policy on overdue and unsettled trades.

Risk Identification

RM-3.1.5 **Investment firm licensees must identify significant concentrations within their asset portfolios. This should be done in relation to:**

(a) Individual counterparties or related groups of counterparties;
(b) Credit ratings of the assets in its portfolio;
(c) The proportion of an issue held;
(d) Instrument types;
(e) Geographical regions; and
(f) Economic sectors.

RM-3.1 Liquidity Risk (continued)

RM-3.1.6 **Investment firm licensees must identify on and off balance sheet impacts on its liquidity.**

RM-3.1.7 For the purposes of RM-3.1.6, the licensee should take into account:

(a) Possible changes in the market's perception of the licensee and the effects that this might have on the licensee's access to the markets, including:
  (i) Where the licensee funds its holdings of assets in one currency with liabilities in another, access to foreign exchange markets, particularly in less frequently traded currencies;
  (ii) Access to secured funding, including by way of repo transactions; and
  (iii) The extent to which the licensee may rely on committed facilities made available to it;

(b) (If applicable) the possible effect of each scenario analysed on currencies whose exchange rates are currently pegged or fixed; and

(c) That:
  (i) General market turbulence may trigger a substantial increase in the extent to which persons exercise rights against the licensee under off balance sheet instruments to which the licensee is party;
  (ii) Access to OTC derivative and foreign exchange markets are sensitive to credit-ratings;
  (iii) The scenario may involve the triggering of early amortisation in asset securitisation transactions with which the licensee has a connection; and
  (iv) Its ability to securitise assets may be reduced at certain times.

Risk Measurement and Monitoring

RM-3.1.8 **An investment firm licensee must establish and maintain a process for the measurement, monitoring and controlling of liquidity risk, using a robust and consistent method which should be described in its liquidity risk policy statement.**

RM-3.1.9 **An investment firm licensee's monitoring framework must include a system of management reporting which provides clear, concise, timely and accurate liquidity risk reports to relevant functions within the firm. These reports must alert management when the investment firm licensee approaches, or breaches, predefined thresholds or limits, including quantitative limits imposed by the CBB.**

RM-3.1 Liquidity Risk (continued)

RM-3.1.10 Reports on liquidity risk should be provided on a timely basis to the investment firm licensee's governing body, senior management and other appropriate personnel. The appropriate content and format of reports depends on a licensee's liquidity management practices and the nature, scale and complexity of the licensee's business. Reports to the investment firm licensee's governing body may be less detailed and less frequent than reports to senior management with responsibility for managing liquidity risk.

RM-3.1.11 For the purposes of testing liquidity risk, licensees must carry out appropriate stress testing and scenario analysis, including taking reasonable steps to identify an appropriate range of realistic adverse circumstances and events in which liquidity risk might occur or crystallise. Licensees should normally consider scenarios based on varying degrees of stress and both firm-specific and market-wide difficulties. In developing any scenario of extreme market-wide stress that may pose systemic risk, it may be appropriate for an investment firm licensee to make assumptions about the likelihood and nature of CBB intervention.

RM-3.1.12 A scenario analysis in relation to liquidity risk should include a cash-flow projection for each scenario tested, based on reasonable estimates of the impact (both on and off balance sheet) of that scenario on the firm's funding needs and sources.

Limit Setting

RM-3.1.13 **Investment firm licensees must set limits in accordance with the nature, scale and complexity of their activities. The structure of limits should reflect the need for investment firm licensees to have systems and controls in place to guard against a spectrum of possible risks, from those arising in day-to-day liquidity risk management to those arising in stressed conditions.**

RM-3.1.14 The CBB would normally expect a licensee to consider setting limits on:

(a) Liability concentrations in relation to:
  (i) Individual, or related groups of, liability providers;
  (ii) Instrument types including those arising from short selling;
  (iii) Maturities, including the amount of debt maturing in a particular period; and
  (iv) Wholesale funding liabilities;
(b) Where appropriate, net leverage and gross leverage; and
(c) Daily settlement limits.

RM-3.1 Liquidity Risk (continued)

Contingency Planning

RM-3.1.15 **Investment firm licensees must maintain contingency funding plans for taking action to ensure, so far as they can, that they can access sufficient liquid financial resources to meet liabilities as they fall due. These plans must also include what events or circumstances may lead to action under the plan being triggered.**

RM-3.1.16 The contingency funding plan should contain administrative policies and procedures that will enable the licensee to manage the plan's implementation effectively, including:

(a) The responsibilities of senior management;
(b) Names and contact details of members of the team responsible for implementing the contingency funding plan;
(c) Where, geographically, team members will be assigned;
(d) Who within the team is responsible for contact with head office (if appropriate), analysts, investors, external auditors, press, significant customers, regulators, lawyers and others; and
(e) Mechanisms that enable senior management and the governing body to receive management information that is both relevant and timely.

RM-4.1 Market Risk

RM-4.1.1 **Investment firm 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-4.1.2 Market risk relates to the exposure of the licensee to fluctuations in the market value, currency or yield in respect of positions in financial instruments (either long or short).

RM-4.1.3 A licensee's market risk policy document should identify its appetite for market risk, systems for identifying, reporting and documenting market risk and mitigation factors in place. In particular, the market risk policy should cover for market risk:

(a) How, with particular reference to its activities, the licensee defines and measures market risk;

(b) The licensee's business aims in incurring market risk including:

(i) Identifying the types and sources of market risk to which the licensee wishes to be exposed (and the limits on that exposure) and those to which the licensee wishes not to be exposed (and how that is to be achieved);

(ii) Specifying the level of diversification required by the licensee and the licensee's tolerance for risk concentrations (and the limits on those exposures and concentrations);

(c) The licensee's investment strategy;

(d) The financial instruments, commodities, assets and liabilities (and mismatches between assets and liabilities) that a licensee is exposed to and the limits on those exposures;

(e) Activities that are intended to hedge or mitigate market risk including mismatches caused by, for example, differences in the assets and liabilities and maturity mismatches; and

(f) The methods and assumptions used for measuring linear, non-linear and geared market risk including the rationale for selection, ongoing validation and testing. Methods might include stress testing and scenario analysis, option Greeks, asset/liability analysis, correlation analysis and Value-at-Risk (VaR). Exposure to non-linear or geared market risk is typically through the use of derivatives.

Risk Identification

RM-4.1.4 **Investment firm licensees must have in place appropriate risk reporting systems that enable them to identify the types and amount of market risk to which they are (or potentially could be) exposed to. The information that systems should capture may include but is not limited to position data which may consist of raw time series of position rates, index levels and prices and derived time series of benchmark yield curves, spreads, implied volatilities, historical volatilities and correlations.**

RM-4.1 Market Risk (continued)

Risk Measurement

RM-4.1.5 **Investment firm licensees must carry out stress testing to access 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 licensee should consider potential market risk events that may affect its solvency. These include the following:

(a) Reduced value 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 of any type (eg. maturity, currency, market, repricing etc.).

RM-4.1.7 Where the licensee considers that the nature of its assets and the matching of its liabilities result in no significant market risk exposure (eg. 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 onsite visit.

Valuation

RM-4.1.8 **Wherever possible, a licensee must mark to market the value of its financial instruments, based on readily available close out prices from independent sources.**

RM-4.1.9 **Where marking to market is not possible, a firm must use mark to model in order to measure the value of its financial instruments. Marking to model is any valuation which has to be benchmarked, extrapolated or otherwise calculated from a market input.**

RM-4.1.10 **A licensee must ensure that its Board of Directors and senior management are aware of the positions which are subject to mark to model and understand the materiality of the uncertainty this creates in the reporting of the performance of the business of the firm and the risks to which it is subject.**

RM-4.1 Market Risk (continued)

RM-4.1.11 **In addition to marking to market or marking to model, a licensee must perform independent price verification, such that market prices or model inputs are regularly verified for accuracy and independence.**

RM-4.1.12 Systems and controls regarding valuations should include the following:

(a) The department responsible for the validation of the value of assets and liabilities should be independent of the business trading area, and should be adequately resourced by suitably qualified staff;

(b) All valuations should be checked and validated at appropriate intervals;

(c) A licensee should establish a review procedure to check :

(i) The quality and appropriateness of the price sources used;

(ii) The level of any valuation reserves held; and

(iii) The valuation methodology employed for each product and consistent adherence to that methodology;

(d) A licensee should document its policies and procedures relating to the entire valuation process. In particular, the following should be documented:

(i) The valuation methodologies employed for all product categories;

(ii) Details of the price sources used for each product;

(iii) The procedures to be followed where a valuation is disputed internally or with a service provider;

(iv) The level at which a difference between a valuation assigned to an asset or liability and the valuation used for validation purposes will be reported on an exceptions basis and investigated;

(v) Where a licensee is using its own internal estimate to produce a valuation, it should document in detail the process followed in order to produce the valuation; and

(vi) The review procedures established by a licensee in relation to the requirements of this section should be adequately documented and include the rationale for the policy.

Risk Monitoring

RM-4.1.13 **The investment firm licensee's risk reporting and monitoring system should be independent of the employees who are responsible for exposing the licensee to risk.**

RM-4.1.14 The market risk policy of a licensee may require the production of market risk reports at various levels within the licensee. These reports should provide sufficiently accurate market risk data to relevant functions within the licensee, and should be timely enough to allow any appropriate remedial action to be proposed and taken, for example:

(a) At firm wide level, a market risk report may include information:

(i) Summarising and commenting on the total market risk that a firm is exposed to and market risk concentrations by business unit, asset class and country;

RM-4.1 Market Risk (continued)

(ii) On VaR calculations, compared to risk limits by business unit, asset class and country;
(iii) Commenting on significant risk concentrations and market developments; and
(iv) On market risk in particular legal entities and geographical regions;

(b) At the business unit level, a market risk report may include information summarising market risk by currency, trading desk, maturity or duration band, or by instrument type;

(c) At the trading desk level, a market risk report may include detailed information summarising market risk by individual trader, instrument, position, currency, or maturity or duration band; and

(d) All risk data should be readily reconcilable back to the prime books of entry with a fully documented audit trail.

RM-4.1.15 **Risk monitoring reports and systems must be subject to periodic independent review by suitably qualified staff.**

Risk Control

RM-4.1.16 Risk control is the independent monitoring, assessment and supervision of business units within the defined policies and procedures of the market risk policy. This may be achieved by:

(a) Setting an appropriate market risk limit structure to control the licensee's exposure to market risk; for example, by setting out a detailed market risk limit structure at the corporate level, the business unit level and the trading desk level which addresses all the key market risk factors and is commensurate with the volume and complexity of activity that the licensee undertakes;

(b) Setting limits on risks such as price or rate risk, as well as those factors arising from options such as delta, gamma, vega, rho and theta;

(c) Setting limits on net and gross positions, market risk concentrations, the maximum allowable loss (also called 'stop-loss'), VaR, potential risks arising from stress testing and scenario analysis, gap analysis, correlation, liquidity and volatility; and

(d) Considering whether it is appropriate to set intermediate (early warning) thresholds that alert management when limits are being approached, triggering review and action where appropriate.

RM-4.1 Market Risk (continued)

Record Keeping

RM-4.1.17 **In relation to market risk, an investment firm licensee must retain appropriate prudential records of:**

(a) [This Subparagraph was deleted in January 2016 and requirements moved to (c)];

(b) The nature and amounts of off and on balance sheet exposures, including aggregations of exposures;

(c) Off and on market trades in financial instruments and other assets and liabilities; and

(d) Methods and assumptions used in stress testing and scenario analysis and in VaR models.

RM-4.1.18 A licensee should keep a data history to enable it to perform back testing of methods and assumptions used for stress testing and scenario analysis and for VaR models.

RM-5.1 Operational Risk

RM-5.1.1 **Investment firm 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-5.1.2 Operational risk is the risk to the licensee of loss resulting from inadequate or failed internal processes, people and systems, or from external events. In identifying the types of operational risk losses that it may be exposed to, licensees should consider, for instance, the following:

(a) The nature of a licensee's customers, products and activities, including sources of business, distribution mechanisms, and the complexity and volumes of transactions;
(b) The design, implementation, and operation of the processes and systems used in the end-to-end operating cycle for a licensee's products and activities;
(c) The risk culture and human resource management practices at a licensee; and
(d) The business operating environment, including political, legal, socio-demographic, technological, and economic factors as well as the competitive environment and market structure.

RM-5.1.3 A licensee should recognise that it may face significant operational exposures from a product or activity that may not be material to its business strategy. A licensee should consider the appropriate level of detail at which risk identification is to take place, and may wish to manage the operational risks that it faces in risk categories that are appropriate to its organisational and legal structures.

RM-5.1.4 **Investment firm licensees must consider the impact of operational risks on their financial resources and solvency.**

RM-5.1.5 **An investment firm licensee's operational risk policy must outline the licensee's strategy and objectives for operational risk management and the processes, including internal controls and risk management mechanisms that it intends to adopt to achieve these objectives.**

RM-5.1.6 When assessing its operational risks, a licensee may be able to differentiate between expected and unexpected operational losses. A licensee should consider whether it is appropriate to adopt a more quantitative approach to the assessment of its expected operational losses, for example by defining tolerance, setting thresholds, and measuring and monitoring operational losses and exposures. In contrast, a licensee may wish to take a more qualitative approach to assessing its unexpected losses.

RM-5.1.7 Although a licensee may currently be unable to assess certain operational risks with a high degree of accuracy or consistency, it should, according to the nature, scale and complexity of its business, consider the use of more sophisticated qualitative and quantitative techniques as they become available.

RM-5.1 Operational Risk (continued)

RM-5.1.8 **Investment firm licensees must establish mechanisms to ensure adequate internal controls are in place.**

RM-5.1.9 For the purposes of RM-5.1.8, internal controls for investment firm licensees should include books and records requirements, appropriate organisation structure, segregation of duties, and related controls that are designed to safeguard entity and client assets.

RM-5.1.10 **Investment firm licensees must establish mechanisms to verify that controls, once established, are being followed. The verification procedures must include internal audits, which must be independent of trading desks and the revenue side of the business.**

RM-5.1.11 In establishing mechanisms and controls, the investment firm licensee should consider:

(a) Corporate structure;
(b) Delegation of authorities;
(c) Outsourcing of functions;
(d) Financial and human resources;
(e) Risk management tools and processes;
(f) Administrative systems and procedures;
(g) Audit trail;
(h) Nature and complexity of client service and fee arrangements;
(i) Investment decision procedures;
(j) Management information systems;
(k) Compliance history and procedures;
(l) Complaints by investors;
(m) Regulatory actions; and
(n) Follow up on regulatory actions and inspection observations.

RM-5.1.12 **Investment firm licensee's 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-5.1.13 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, investment firm licensees cannot ignore the nature of risks to which they are exposed.

RM-5.1 Operational Risk (continued)

Risk Monitoring and Controlling

RM-5.1.14 **When monitoring their operational risk, investment firm licensees must:**

(a) Report regularly to the relevant level of management its operational exposures, loss experience (including if possible cumulative losses), and authorised deviations from the investment firm licensee's operational risk policy;

(b) Engage in exception-based escalation to management of:

(i) Unauthorised deviations from the investment firm licensee's operational risk policy;

(ii) Likely or actual breaches in predefined thresholds for operational exposures and losses, where set; and

(iii) Significant increases in the investment firm licensee's exposure to operational risk or alterations to its operational risk profile.

Record Keeping

RM-5.1.15 **Investment firm licensees must retain an appropriate record of their operational risk management activities.**

RM-5.1.16 RM-5.1.15 may, for example, include records of:

(a) The results of risk identification, measurement, and monitoring activities;
(b) Actions taken to control identified risks;
(c) Where relevant, any exposure thresholds that have been set for identified operational risks;
(d) An assessment of the effectiveness of the risk control tools that are used; and
(e) Actual operational risk losses or events against stated risk appetite or tolerance.

RM-6.1 Derivative Transactions Risk

RM-6.1.1 **Investment firm licensees must seek prior CBB approval before starting to undertake derivative transactions. Investment firm licensees that engage in derivatives trading for their own account or for clients must evaluate the systems needs for such activity.**

RM-6.1.2 Rule RM-6.1.1 requires a one-off approval, before undertaking derivatives activity, rather than approval for each such transaction. With the complexity of derivatives products and the size and rapidity of transactions, it is essential that licensees capture all relevant details of transactions, identify errors and process payments or move assets quickly and accurately. This requires a staff of sufficient size, knowledge and experience to support the volume and type of transactions.

RM-6.1.3 Current and projected volumes should be considered together with the nature of the derivatives activity and the users' expectations. Consistent with other systems plans, a written contingency plan for derivative products should be in place.

RM-6.1.4 **Investment firm licensees must ensure that a mechanism exists whereby derivatives contract documentation is confirmed, maintained and safeguarded.**

RM-6.1.5 Investment firm licensees should establish a process through which documentation exceptions are monitored and resolved and appropriately reviewed by senior management and legal counsel.

RM-6.1.6 The licensee should also have approved policies that specify documentation requirements for derivatives activities and formal procedures for saving and safeguarding important documents that are consistent with legal requirements and internal policies.

RM-6.1.7 **Investment firm licensees must have adequate systems support and operational capacity to accommodate the types of derivatives activities in which it engages.**

RM-6.1.8 Systems design and needs may vary according to the size and complexity of the derivatives business. However, each system should provide for accurate and timely processing and allow for proper risk exposure monitoring. Operational systems should be tailored to each licensee's needs. Limited end-users of derivatives may not require the same degree of automation needed by more active trading institutions. All operational systems and units should adequately provide for basic processing, settlement and control of derivatives transactions.

RM-6.1 Derivative Transactions Risk (continued)

RM-6.1.9 For the purposes of RM-6.1.7, the systems should consider:

(a) The firm's ability to efficiently process and settle the volumes of transactions;
(b) The firm's ability to monitor and predict margin calls and settlement calls;
(c) Availability of data sets including statistical factors particularly in respect of derivatives (betas, gammas etc.);
(d) Processes to ensure that the data sets used are current and subject to validation processes to provide support for the complexity of the transaction booked;
(e) The integrity of the valuation models used for derivative transactions – the investment firm licensee should have appropriate policies and processes ensuring accuracy and completeness of the related data flows including the data sets mentioned above, stress testing, backtesting for ensuring; and
(f) Support systems and the systems developed to interface with the core applications or databases should generate accurate information sufficient and to allow business unit management and senior management to monitor risk exposures in a timely manner.

RM-6.1.10 The more sophisticated the licensee's activity, the more need there is to establish automated systems to accommodate the complexity and volume of the deals transacted, to report position data accurately and to facilitate efficient reconciliation.

RM-7.1 Outsourcing Risk

RM-7.1.1 **Investment firm licensees must identify all material outsourcing contracts and ensure that the risks associated with such contracts are adequately controlled. In particular, investment firm licensees must comply with the specific requirements set out in this Chapter.**

RM-7.1.2 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-7.1.3 For purposes of RM-7.1.1, 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 clients. 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-7.1.3A 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-7.1.4 **Investment firm 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-7.1.5 **Investment firm 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-7.1.6 **Investment firm licensees must seek the CBB's prior written approval before committing to a new material outsourcing arrangement.**

RM-7.1.7 **Investment firm licensees may not outsource their core business function or activities to third parties.**

RM-7.1 Outsourcing Risk (continued)

Supervisory Approach (continued)

RM-7.1.8 **The prior approval request in RM-7.1.6 must:**

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

(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-7.1.9 The CBB will review the information provided and provide a definitive response within a reasonable period of time of receiving the request for approval referred to in Paragraph RM-7.1.8. The CBB may also contact home or host supervisors to seek their comments – in such cases, the period of time is also subject to the speed of their response.

RM-7.1.9A The CBB's approach to approving requests for outsourcing arrangements will also consider whether the investment firm licensee has engaged in considerable outsourcing of its activities, a practice which the CBB does not favour.

RM-7.1.10 **Once an activity has been outsourced, a licensee must continue to monitor the associated risks and the effectiveness of its mitigating controls.**

RM-7.1.11 **Investment firm 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 investment firm licensee to make alternative arrangements for the outsourced activity.**

RM-7.1.11A 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-7.1.12 **The CBB requires ongoing access to the outsourced activity, which it may occasionally want to examine itself, through management meetings or on-site examinations.**

RM-7.1 Outsourcing Risk (continued)

Supervisory Approach (continued)

Risk Assessment

RM-7.1.13 **Investment firm 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-7.1.14 Before entering into, or significantly changing, an outsourcing arrangement, a licensee should:

(a) Analyse how the arrangement will fit with its organisation and reporting structure; business strategy; overall risk profile; and ability to meet its regulatory obligations;
(b) Consider whether the agreements establishing the arrangement will allow it to monitor and control its operational risk exposure relating to the outsourcing;
(c) Conduct appropriate due diligence of the service provider's financial stability and expertise;
(d) Consider how it will ensure a smooth transition of its operations from its current arrangements to a new or changed outsourcing arrangement (including what will happen on the termination of the contract);
(e) Consider any concentration risk implications such as the business continuity implications that may arise if a single service provider is used by several firms; and
(f) Analyse 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.

RM-7.1.15 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 client 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

RM-7.1 Outsourcing Risk (continued)

(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-7.1.16 **Investment firm 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-7.1 Outsourcing Risk (continued)

RM-7.1.17 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 written prior approval required under Rule RM-7.1.6. Any subsequent replacement of such person must also be notified to the CBB.

RM-7.1.18 All material outsourcing arrangements by an investment firm licensee 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 client 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.

RM-7.2 Outsourcing Agreement

RM-7.2.1 **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-7.2.2 **The Board and management of licensees are held ultimately responsible by the CBB for the adequacy of systems and controls in outsourced activities. Investment firm licensees must therefore ensure they have adequate mechanisms for monitoring the performance of, and managing the relationship with, the outsourcing provider.**

RM-7.2.3 Clear reporting and escalation mechanisms must be specified in the agreement.

RM-7.2.4 **Where an outsourcing provider in turn decides to sub-contract to other providers, CBB 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.**

Customer Data Confidentiality

RM-7.2.5 **Investment firm licensees must ensure that outsourcing agreements comply with all applicable legal requirements regarding client confidentiality.**

RM-7.2.6 **Investment firm licensees must ensure that the outsourcing provider implements adequate safeguards and procedures.**

RM-7.2.7 For the purposes of RM-7.2.6, the implementation of adequate safeguards would include the proper segregation of client 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 breach of confidentiality.

RM-7.2.8 **Investment firm 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-7.2 Outsourcing Agreement (continued)

RM-7.2.9 Investment firm 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-7.2.10 Outsourcing agreements must ensure that the investment firm 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-7.2.11 Investment firm 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-7.2.12 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 RM-7.2.10 and RM-7.2.11 above. Should such restrictions be imposed, the licensee must communicate this fact to the CBB as soon as it becomes aware of the matter.

RM-7.2.13 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-7.2.14 Investment firm licensees must ensure that service providers maintain, regularly review and test plans to ensure continuity in the provision of the outsourced service.

RM-7.2 Outsourcing Agreement (continued)

RM-7.2.15 Investment firm 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-7.2.16 Investment firm 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-7.2.17 Termination under any other circumstances allowed under the agreement must give investment firm 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-7.2.18 In the event of termination, for whatever reason, the agreement must provide for the return of all client data – where required by investment firm licensees – or destruction of the records.

Cloud services

RM-7.2.19 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;

RM-7.2 Outsourcing Agreement (continued)

RM-7.2.19

(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-7.3 Intra-group Outsourcing

RM-7.3.1 **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-7.3.2 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-7.3.3 **Investment firm licensees 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-7.3.4 The CBB will respond to the request for approval in Paragraph RM-7.3.3 in the same manner and timescale as set out in Paragraph RM-7.1.9 and will also consider the issue of considerable outsourcing as outlined in Paragraph RM-7.1.9A.

RM-7.3.5 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-7.3.6 The CBB also expects a licensee's management to have addressed the issues of customer confidentiality, access to information and business continuity.

RM-7.3.7 **Investment firm 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-7.4 Internal Audit Outsourcing

RM-7.4.1 **Licensees may not outsource their internal audit function to the same firm that acts as their external auditors.**

RM-7.4.2 **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-7.4.2A **All requests to outsource the internal audit function must be supported by a board resolution or ratified by the audit committee.**

RM-7.4.3 **The CBB will only consider a licensee not having a separate internal audit function where its activities are limited in scale and complexity. In such case, it may continue to outsource this function for a period determined by the CBB.**

RM-7.4.4 **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.**

RM-7.4.5 Due to 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-8.1 Group Risk

RM-8.1.1 **Section RM-8.1 applies only to Bahraini investment firm licensees.**

RM-8.1.2 **Investment firm licensees must identify, manage and control risks to their 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 licensee should it have reason to believe that other members of the group pose undue risk to the 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 the 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 required to request sufficient information of its group members to allow it to address group risks.**

Systems and Controls

RM-8.1.6 **The investment firm licensee must have adequate, sound and appropriate risk management processes and internal control mechanisms for the purpose of assessing and managing its own exposure to group risk, including sound administrative and accounting procedures.**

RM-8.1.7 For the purposes of RM-8.1.6, the question of whether the risk management processes and internal control mechanisms are adequate, sound and appropriate should be judged in the light of the nature, scale and complexity of the group's business and the level of interaction between the investment firm and the group.

RM-8.1.8 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 financial position of the group. This should be evidenced in the prudential records retained in Bahrain.

RM-8.1 Group Risk (continued)

RM-8.1.9 **The internal control mechanisms referred to in RM-8.1.6 must include:**

(a) Mechanisms that are adequate for the purpose of producing any data and information which would be relevant for the purpose of monitoring compliance with any prudential requirements (including any reporting requirements and any requirements relating to capital adequacy, solvency and large exposures):

(i) To which the investment firm licensee is subject with respect to its membership of a group; or

(ii) That apply to or with respect to that group or part of it; and

(b) Mechanisms that are adequate to monitor funding within the group.

RM-8.1.10 **In assessing group risk systems and controls, the investment firm 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 the linkages between group and 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-8.1.11 A 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 within the group should be clearly documented.

Reporting Requirement

RM-8.1.12 **Where the investment firm licensee's group or parent reports its own capital adequacy 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.**

RM-9.1 Cyber Security Risk Measures

RM-9.1.1 Investment firm 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.

RM-9.1.2 Overseas investment firm licensees should confirm in writing to the CBB that policies covering all requirements of this Chapter are in place at the head office level.

Training

RM-9.1.3 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. The effectiveness of the training should be tested on a periodic basis such as through testing employee reactions to simulated cyber-attack scenarios. The results of such tests must be used to further enhance the cyber security training of employees. All relevant employees must be informed on the current cyber security breaches and threats.

Role of Board and Senior Management

RM-9.1.4 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-9.1.5 The Board of the investment firm 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) Ensure that cyber roles withing 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 managemnet; and
e) Receiving reports on all cyber incidents.

RM-9.1 Cyber Security Risk Measures (continued)

RM-9.1.6 The senior management of an investment firm licensee must be responsible for the following activities:

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

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

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

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

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

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

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

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

RM-9.1.7 The senior management of an investment firm licensee is responsible for monitoring the implementation of any cyber security related outstanding issues through progress reports at regular intervals.

RM-9.1.8 Cyber security risk must be an item for discussion at Board meetings.

RM-9.1.9 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-9.1.10 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-9.1.11 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 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-9.1.12 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 securityrisk 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 indexes; and
f) Evaluation, control and reporting.

RM-9.1.13 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 lifecycle 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-9.1.14 Licensees must arrange to seek cyber security risk insurance cover from a suitable 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; and

c) Policy also provides 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-9.1.15 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-9.1.16 Licensees must report to the CBB and Ministry of Interior's General Directorate of Anti-Corruption and Economic and Electronic Security any instances of cyber-attacks immediately, whether internal or external, that compromise customer information or disrupt critical services that affect their operations. When reporting such instances, licensees must provide the root cause analysis of the cyber-attack and measures taken by them to ensure that similar events do not recur. 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-9.1.17 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 auditors or consultants.

RM-9.1.18 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.