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	04/2019	Added a new Chapter on Cyber Security Risk.
RM-9.1	01/2022	Enhanced Section on Cyber Security Risk Management.
RM-9.1.58	04/2022	Amended Paragraph on the cyber security reporting.
RM-9.1.59	04/2022	Amended Paragraph on the submission of the cyber security report.
RM-7	07/2022	Replaced Chapter RM-7 with new Outsourcing Requirements.

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 Arrangements

RM-7.1.1 **This Chapter sets out the CBB's approach to outsourcing by licensees. It also sets out various requirements that licensees must address when considering outsourcing an activity or function.**

RM-7.1.2 In the context of this Chapter, 'outsourcing' means an arrangement whereby a third party performs on behalf of a licensee an activity which commonly 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 In the case of branches of foreign entities, the CBB may consider a third-party outsourcing arrangement entered into by the licensee's head office/regional office or other offices of the foreign entity as an intragroup outsourcing, provided that the head office/regional office submits to the CBB a letter of comfort which includes, but is not limited to, the following conditions:

i. The head office/regional office declares its ultimate responsibility of ensuring that adequate control measures are in place; and

ii. The head office/regional office is responsible to take adequate rectification measures, including compensation to the affected customers, in cases where customers suffer any loss due to inadequate controls applied by the third-party service provider.

RM-7.1.4 **The licensee must not outsource the following functions:**

(i) Compliance;

(ii) AML/CFT;

(iii) Financial control;

(iv) Risk management; and

(v) Business line functions offering regulated services directly to the customers (refer to Regulation No. (1) of 2007 and its amendments for the list of CBB regulated services).

RM-7.1.5 **For the purposes of Paragraph RM-7.1.4, certain support activities, processes and systems under these functions may be outsourced (e.g. call centres, data processing, credit recoveries, cyber security, e-KYC solutions) subject to compliance with Paragraph RM-7.1.7. However, strategic decision-making and managing and bearing the principal risks related to these functions must remain with the licensee.**

RM-7.1.6 Branches of foreign entities may be allowed to outsource to their head office, the risk management function stipulated in Subparagraph RM-7.1.4 (iv), subject to CBB's prior approval.

RM-7.1 Outsourcing Arrangements (continued)

RM-7.1.7 Licensees must comply with the following requirements:

(i) Prior CBB approval is required on any outsourcing to a third-party outside Bahrain (excluding cloud data services). The request application must:

a. include information on the legal and technical due diligence, risk assessment and detailed compliance assessment; and

b. be made at least 30 calendar days before the licensee intends to commit to the arrangement.

(ii) Post notification to the CBB, within 5 working days from the date of signing the outsourcing agreement, is required on any outsourcing to an intragroup entity within or outside Bahrain or to a third-party within Bahrain, provided that the outsourced service does not require a license, or to a third-party cloud data services provider inside or outside Bahrain.

(iii) Licensees must have in place sufficient written requirements in their internal policies and procedures addressing all strategic, operational, logistical, business continuity and contingency planning, legal and risks issues in relation to outsourcing.

(iv) Licensees must sign a service level agreement (SLA) or equivalent with every outsourcing service provider. The SLA must clearly address the scope, rights, confidentiality and encryption requirements, reporting and allocation of responsibilities. The SLA must also stipulate that the CBB, external auditors, internal audit function, compliance function and where relevant the Shari'a coordination and implementation and internal Shari'a audit functions of the licensee have unrestricted access to all relevant information and documents maintained by the outsourcing service provider in relation to the outsourced activity.

(v) Licensees must designate an approved person to act as coordinator for monitoring and assessing the outsourced arrangement.

(vi) Licensee must submit to the CBB any report by any other regulatory authority on the quality of controls of an outsourcing service provider immediately after its receipt or after coming to know about it.

(vii) Licensee must inform its normal supervisory point of contact at the CBB of any material problems encountered with the outsourcing service provider if they remain unresolved for a period of three months from its identification date.

RM-7.1 Outsourcing Arrangements (continued)

RM-7.1.8 For the purpose of Subparagraph RM-7.1.7 (iv), licensees as part of their assessments may use the following:

a) Independent third-party certifications on the outsourcing service provider's security and other controls;
b) Third-party or internal audit reports of the outsourcing service provider; and
c) Pooled audits organized by the outsourcing service provider, jointly with its other clients.

When conducting on-site examinations, licensees should ensure that the data of the outsourcing service provider's other clients is not negatively impacted, including impact on service levels, availability of data and confidentiality.

RM-7.1.9 For the purpose of Subparagraph RM-7.1.7 (i), the CBB will provide a definitive response to any prior approval request for outsourcing within 10 working days of receiving the request complete with all the required information and documents.

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.**

MODULE	RM:	Risk Management
CHAPTER	RM-7:	Group Risk

MODULE	RM:	Risk Management
CHAPTER	RM-9:	Cyber Security Risk Management

RM-9.1 Cyber Security Risk Management

Role of the Board and Senior Management

RM-9.1.1 **The Board of investment firm licensees must ensure that the licensee has a robust cyber security risk management framework to comprehensively manage the licensee's cyber security risk and vulnerabilities. The Board must establish clear ownership, decision-making and management accountability for risks associated with cyber-attacks and related risk management and recovery processes.**

RM-9.1.2 **Licensees must ensure that the cyber security risk management framework encompasses, at a minimum, the following components:**

a) Cyber security strategy;
b) Cyber security policy; and
c) Cyber security risk management approach, tools and methodology and, an organization-wide security awareness program.

RM-9.1.3 **The cyber security risk management framework must be developed in accordance with the National Institute of Standards and Technology (NIST) Cyber security framework which is summarized in Appendix A – Cyber security Control Guidelines. At the broader level, the Cyber security framework should be consistent with the licensee's risk management framework.**

RM-9.1.4 Senior management, and where appropriate, the board should receive comprehensive reports covering cyber security issues such as the following:

a. Key Risk Indicators/ Key Performance Indicators;
b. Status reports on overall cyber security control maturity levels;
c. Status of staff Information Security awareness;
d. Updates on latest internal or relevant external cyber security incidents; and
e. Results from penetration testing exercises.

RM-9.1.5 **The Board must ensure that the cyber security risk management framework is evaluated for scope of coverage, adequacy and effectiveness every three years or when there are significant changes to the risk environment, taking into account emerging cyber threats and cyber security controls.**

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.6 **Licensees must have in place arrangements, commensurate with their size and risk profile, to handle cyber security risk management responsibilities. Licensees may assign the responsibilities to a qualified Chief Information Security Officer (CISO) reporting to an independent risk management function or incorporate the responsibilities of cyber security risk into the risk management function. Overseas investment firm licensees must be governed under a framework of cyber security risk management policies which ensure that an adequate level of oversight is exercised by the regional office or head office.**

RM-9.1.7 Licensees should ensure that appropriate resources are allocated to the cyber security risk management function for implementing the cyber security framework.

RM-9.1.8 **Licensees must ensure that the cyber security risk management function is headed by suitably qualified Chief Information Security Officer (CISO), with appropriate authority to implement the Cyber Security strategy.**

RM-9.1.9 Licensees may establish a cyber security committee that is headed by an independent senior manager from a control function (like CFO / CRO), with appropriate authority to approve policies and frameworks needed to implement the cyber security strategy, and act as a governance committee for the cyber security function. Membership of this committee should include senior management members from business functions, IT, Risk and Compliance.

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.10 The senior management must be responsible for the following activities:

(a) Create the overall cyber security risk management framework and adequately oversee its implementation;
(b) Formulate an organisation-wide cyber security strategy and cyber security policy;
(c) Implement and consistently maintain an integrated, organisation-wide, cyber security risk management framework, and ensure sufficient resource allocation;
(d) Monitor the effectiveness of the implementation of cyber security risk management practices and coordinate cyber security activities with internal and external risk management entities;
(e) Ensure that internal management reporting caters to cyber threats and cyber security risk treatment;
(f) Prepare quarterly or more frequent reports on all cyber incidents (internal and external) and their implications on the licensee; and
(g) Ensure that processes for identifying the cyber security risk levels across the licensee are in place and annually evaluated.

RM-9.1.11 The senior management must ensure that:

(a) The licensee has identified clear internal ownership and classification for all information assets and data;
(b) The licensee has maintained an inventory of the information assets and data which is reviewed and updated regularly;
(c) The cyber security staff are adequate to manage the licensee's cyber security risks and facilitate the performance and continuous improvement of all relevant cyber security controls;
(d) It provides and requires cyber security staff to attend regular cyber security update and training sessions (for example Security+, CEH, CISSP, CISA, CISM, CCSP) to stay abreast of changing cyber security threats and countermeasures.

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.12 With respect to Subparagraph RM-9.1.11(a), data classification entails analyzing the data the licensee retains, determining its importance and value, and then assigning it to a category. When classifying data, the following aspects of the policy should be determined:

a) Who has access to the data;
b) How the data is secured;
c) How long the data is retained (this includes backups);
d) What method should be used to dispose of the data;
e) Whether the data needs to be encrypted; and
f) What use of the data is appropriate.

The general guideline for data classification is that the definition of the classification should be clear enough so that it is easy to determine how to classify the data. In other words, there should be little (if any) overlap in the classification definitions. The owner of data (i.e. the relevant business function) should be involved in such classification.

Cyber Security Strategy

RM-9.1.13 **An organisation-wide cyber security strategy must be defined and documented to include:**

(a) The position and importance of cyber security at the licensee;
(b) The primary cyber security threats and challenges facing the licensee;
(c) The licensee's approach to cyber security risk management;
(d) The key elements of the cyber security strategy including objectives, principles of operation and implementation approach;
(e) Scope of risk identification and assessment, which must include the dependencies on third party service providers;
(f) Approach to planning response and recovery activities; and
(g) Approach to communication with internal and external stakeholders including sharing of information on identified threats and other intelligence among industry participants.

RM-9.1.14 The cyber security strategy should be communicated to the relevant stakeholders and it should be revised as necessary and, at least, once every three years. Appendix A provides cyber security control guidelines that can be used as reference to support the licensee's cyber security strategy and cyber security policy.

RM-9.1 Cyber Security Risk Management (continued)

Cyber Security Policy

RM-9.1.15 Licensees must implement a written cyber security policy setting forth its policies for the protection of its electronic systems and client data stored on those systems, which must be reviewed and approved by the licensee's senior management, as appropriate, at least annually. The cyber security policy areas including but not limited to the following must be addressed:

(a) Definition of the key cyber security activities within the licensee, the roles, responsibilities, delegated powers and accountability for these activities;

(b) A statement of the licensee's overall cyber risk tolerance as aligned with the licensee's business strategy. The cyber risk tolerance statement should be developed through consideration of the various impacts of cyber threats including customer impact, service downtime, potential negative media publicity, potential regulatory penalties, financial loss, and others;

(c) Definition of main cyber security processes and measures and the approach to control and assessment;

(d) Policies and procedures (including process flow diagrams) for all relevant cyber security functions and controls including the following:

(a) Asset management (Hardware and software);
(b) Incident management (Detection and response);
(c) Vulnerability management;
(d) Configuration management;
(e) Access management;
(f) Third party management;
(g) Secure application development;
(h) Secure change management;
(i) Cyber training and awareness;
(j) Cyber resilience (business continuity and disaster planning); and
(k) Secure network architecture.

RM-9.1 Cyber Security Risk Management (continued)

Approach, Tools and Methodology

RM-9.1.16 **Licensees must ensure that the cyber security policy is effectively implemented through a consistent risk-based approach using tools and methodologies that are commensurate with the size and risk profile of the licensee. The approach, tools and methodologies must cover all cyber security functions and controls defined in the cyber security policy.**

RM-9.1.17 Licensees should establish and maintain plans, policies, procedures, process and tools ("playbooks") that provide well-defined, organised approaches for cyber incident response and recovery activities, including criteria for activating the measures set out in the plans and playbooks to expedite the licensee's response time. Plans and playbooks should be developed in consultation with business lines to ensure business recovery objectives are met and are approved by senior management before broadly shared across the licensee. They should be reviewed and updated regularly to incorporate improvements and/or changes in the licensee. Licensees may enlist external subject matter experts to review complex and technical content in the playbook, where appropriate. A number of plans and playbooks should be developed for specific purposes (e.g. response, recovery, contingency, communication) that align with the overall cyber security strategy.

Prevention Controls

RM-9.1.18 **A Licensee must develop and implement preventive measures across all relevant technologies to minimise the licensee's exposure to cyber security risk. Such preventive measures must include, at a minimum, the following:**

(a) Deployment of End Point Protection (EPP) and Endpoint Detection and Response (EDR) including anti-virus software and anti-malware programs to detect, prevent, and isolate malicious code;

(b) Use of firewalls for network segmentation including use of Web Application Firewalls (WAF) where relevant, for filtering and monitoring HTTP traffic between a web application and the Internet, and access control lists to limit unauthorized system access between network segments;

(c) Rigorous security testing at software development stage as well as after deployment to limit the number of vulnerabilities;

(d) Use of a secure email gateway to limit email based cyber attacks such as malware attachments, malicious links, and phishing scams (for example use of Microsoft Office 365 Advanced Threat Protection tools for emails);

RM-9.1 Cyber Security Risk Management (continued)

(e) Use of a Secure Web Gateway to limit browser based cyber-attacks, malicious websites and enforce organization policies;

(f) Creating a list of whitelisted applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on the organization's systems; and

(g) Implementing Bring Your Own Device "BYOD" security policies to secure all mobile devices with any access to licensee systems, applications, and networks through security measures such as encryption, remote wipe capabilities, and password enforcement.

RM-9.1.19 Licensees should also implement the following prevention controls in the following areas:

(a) Data leakage prevention to detect and prevent confidential data from leaving the licensee's technology environment;

(b) Controls or solutions to secure, control, manage and monitor privileged access to critical assets, (e.g. Privileged Access Management (PAM);

(c) Controls to secure physical network ports against connection to computers which are unauthorised to connect to the licensee's network or which do not meet the minimum-security requirements defined for licensee computer systems (e.g. Network access control); and

(d) Identity and access management controls to limit the exploitation and monitor the use of privileged and non-privileged accounts.

RM-9.1.20 Licensees must set up anti-spam and anti-spoofing measures to authenticate the licensee's mail server and to prove to ISPs, mail services and other receiving mail servers that senders are truly authorized to send the email. Examples of such measures include:

- **SPF "Sender Policy Framework";**
- **DKIM "Domain Keys Identified Mail"; and**
- **DMARC "Domain-based Message Authentication, Reporting and Conformance".**

RM-9.1.21 Licensees should subscribe to one of the Cyber Threat Intelligence services in order to stay abreast of emerging cyber threats, cybercrime actors and state of the art tools and security measures.

RM-9.1.22 Licensees must use a single unified email domain for communication with customers to prevent abuse by third parties. For example, ensuring that all emails are sent from xyz@licensee.com and not utilizing shortened services or third-party email providers. Licensees must not use URLs in SMS or other short messages.

RM-9.1 Cyber Security Risk Management (continued)

Cyber Risk Identification and Assessments

RM-9.1.23 **Licensees must conduct periodic assessments of cyber threats. For the purpose of analysing and assessing current cyber threats relevant to the licensee, it should take into account the factors detailed below:**

(a) Cyber threat entities including cyber criminals, cyber activists, insider threats;

(b) Methodologies and attack vectors across various technologies including cloud, email, websites, third parties, physical access, or others as relevant;

(c) Changes in the frequency, variety, and severity of cyber threats relevant to the region;

(d) Dark web surveillance to identify any plot for cyber attacks;

(e) Examples of cyber threats from past cyber attacks on the licensee if available; and

(f) Examples of cyber threats from recent cyber attacks on other organisations.

RM-9.1.24 **Licensees must conduct periodic assessments of the maturity, coverage, and effectiveness of all cyber security controls. Cyber security control assessment must include an analysis of the controls' effectiveness in reducing the likelihood and probability of a successful attack.**

RM-9.1.25 Licensees should ensure that the periodic assessments of cyber threats and cyber security controls cover all critical technology systems. A risk treatment plan should be developed for all residual risks which are considered to be above the licensee's risk tolerance levels.

RM-9.1.26 **Licensees must conduct regular technical assessments to identify potential security vulnerabilities for systems, applications, and network devices. The vulnerability assessments must be comprehensive and cover internal technology, external technology, and connections with third parties. Assessments for external public facing services and systems must be more frequent.**

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.27 With respect to Paragraph RM-9.1.26, external technology refers to the licensee's public facing technology such as websites, apps and external servers. Connections with third parties includes any API or other connections with fintech companies, technology providers, outsourcing service providers etc.

RM-9.1.28 **Licensees must have in place vulnerability and patch management processes which include remediation processes to ensure that the vulnerabilities identified are addressed and that security patches are applied where relevant within a timeframe that is commensurate with the risks posed by each vulnerability.**

RM-9.1.29 **All licensees must perform penetration testing of their systems, applications, and network devices to verify the robustness of the security controls in place at least once a year. These tests must be used to simulate real world cyber-attacks on the technology environment and must:**

(a) Follow a risk-based approach based on an internationally recognized methodology, such as National Institute of Standards and Technology "NIST" and Open Web Application Security Project "OWASP";
(b) Include both Grey Box and Black Box testing in its scope;
(c) Be conducted by qualified and experienced security professionals who are certified in providing penetration testing services;
(d) Be performed by internal and external independent third parties which should be changed at least every two years; and
(e) Be performed on either the production environment or on non-production exact replicas of the production environment.

RM-9.1.30 CBB may require additional third-party security reviews to be performed as needed.

RM-9.1.31 **The tests referred to in Paragraph RM-9.1.29 must be conducted each year in June and the report on such testing must be submitted to the CBB before 30th September. The penetration testing reports must include the vulnerabilities identified and a full list of 'passed' tests and 'failed' tests together with the steps taken to mitigate the risks identified.**

RM-9.1 Cyber Security Risk Management (continued)

Cyber Incident Detection and Management

RM-9.1.32 **Licensees must implement cyber security incident management processes to ensure timely detection, response and recovery for cyber security incidents. This includes implementing a monitoring system for log correlation and anomaly detection.**

RM-9.1.33 Licensees should receive data on a real time basis from all relevant systems, applications, and network devices including operational and business systems. The monitoring system should be capable of identifying indicators of cyber incidents and initiate alerts, reports, and response activities based on the defined cyber security incident management process.

RM-9.1.34 Licensees should retain the logs and other information from the monitoring system for detecting cyber incidents, including "low-and-slow" attacks, in order to facilitate incident investigations, for 12 months or longer.

RM-9.1.35 Once a cyber incident is detected, licensees should activate their containment measures, processes and technologies best suited to each type of cyber incident to prevent a cyber incident from inflicting further damage. This may involve, after considering the costs, business impact and operational risks, shutting down or isolating all or affected parts of their systems and networks as deemed necessary for containment and diagnosis.

RM-9.1.36 **Licensees must define roles and responsibilities and assign adequate resources to detect, identify, investigate and respond to cyber incidents that could impact the licensee's infrastructure, services and customers. Such responsibilities must include log correlation, anomaly detection and maintaining the licensee's asset inventory and network diagrams.**

RM-9.1.37 **Licensees must regularly identify, test, review and update current cyber security risk scenarios and the corresponding response plan. This is to ensure that the scenarios and response plan remain relevant and effective, taking into account changes in the operating environment, systems or the emergence of new cyber security threats. If any gaps are identified, the monitoring system must be updated with new use cases and rule sets which are capable of detecting the current cyber incident scenarios.**

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.38 The cyber incident scenario tests should include high-impact-low-probability events and scenarios that may result in failure. Common cyber incident scenarios include distributed denial of service (DDoS) attacks, system intrusion, data exfiltration and system disruption. Licensees should regularly use threat intelligence to update the scenarios so that they remain current and relevant. Licensees should periodically review current cyber incident scenarios for the purpose of assessing the licensee's ability to detect and respond to these scenarios if they were to occur.

RM-9.1.39 **Licensees must ensure that critical cyber security incidents detected are escalated to an incident response team, management and the Board, in accordance with the licensee's business continuity plan and crisis management plan, and that an appropriate response is implemented promptly. See also Paragraph RM-9.1.58 for the requirement to report to CBB.**

RM-9.1.40 Licensees should clearly define the roles, responsibilities and accountabilities for cyber incident detection and response activities to one or more named individuals that meet the pre-requisite role requirements. Potential conflicts of interest are minimised by ensuring a separation of implementation and oversight roles where possible. The roles should include:

- **Incident Owner:** An individual that is responsible for handling the overall cyber incident detection and response activities according to the incident type and services affected. The Incident Owner is delegated appropriate authority to manage the mitigation or preferably, removal of all impacts due to the incident.
- **Spokesperson:** An individual, from External Communications Unit or another suitable department, that is responsible for managing the communications strategy by consolidating relevant information and views from subject matter experts and the licensee's management to update the internal and external stakeholders with consistent information.
- **Record Keeper:** An individual that is responsible for maintaining an accurate record of the cyber incident throughout its different phases, as well as documenting actions and decisions taken during and after a cyber incident. The record serves as an accurate source of reference for after-action reviews to improve future cyber incident detection and response activities.

RM-9.1.41 For the purpose of managing a critical cyber incident, the licensee should operate a situation room, and should include in the incident management procedure a definition of the authorities and responsibilities of staff members, internal and external reporting lines, communication channels, tools and detailed working procedures. The situation room or a war room is a physical room or a virtual room where relevant members of the management gather to handle a crisis in the most efficient manner possible.

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.42 Licensees should record and document in an orderly manner the incidents that have been handled and the actions that were taken by the relevant functions. In particular, the licensee should maintain an "incident log" in which all the notifications, decisions and actions taken, in relation to cyber incidents, are documented, as close as possible to the time of their occurrence. It should also include the status of the issue whether it is open or has been resolved and person in charge of resolving the issue/incident. The logs should be stored and preserved in a secure and legally admissible manner.

RM-9.1.43 Licensees should utilise pre-defined taxonomy for classifying cyber incidents according to, for example, the type of incident, threat actors, threat vectors and repercussions; and a pre-established severity assessment framework to help gauge the severity of the cyber incident. For example, taxonomies that can be used when describing cyber incidents:

(a) Describe the cause of the cyber incident (e.g. process failure, system failure, human error, external event, malicious action)
(b) Describe whether the cyber incident due to a third-party service provider
(c) Describe the attack vector (e.g. malware, virus, worm, malicious hyperlink)
(d) Describe the delivery channel used (e.g. e-mail, web browser, removable storage media)
(e) Describe the impact (e.g. service degradation/disruption, service downtime, potential impact to customers, data leakage, unavailability of data, data destruction/corruption, tarnishing of reputation)
(f) Describe the type of incident (e.g. zero-day attack, exploiting a known vulnerability, isolated incident)
(g) Describe the intent (e.g. malicious, theft, monetary gain, fraud, political, espionage, opportunistic)
(h) Describe the threat actor (e.g. script kiddies, amateur, criminal syndicate, hacktivist, nation state)

The cyber incident severity may be classified as:

(a) **Severity 1** incident has or will cause a serious disruption or degradation of critical service(s) and there is potentially high impact on public confidence in the licensee.
(b) **Severity 2** incident has or will cause some degradation of critical services and there is medium impact on public confidence in the licensee.
(c) **Severity 3** incident has little or no impact to critical services and there is no visible impact on public confidence in the licensee.

RM-9.1.44 Licensees should determine the effects of the cyber incident on customers and to the wider financial system as a whole and report the results of such an assessment to CBB if it is determined that the cyber incident may have a systemic impact.

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.45 Licensees should establish metrics to measure the impact of a cyber incident and to report to management the performance of response activities. Examples include:

1. Metrics to measure impact of a cyber incident
   (a) Duration of unavailability of critical functions and services
   (b) Number of stolen records or affected accounts
   (c) Volume of customers impacted
   (d) Amount of lost revenue due to business downtime, including both existing and future business opportunities
   (e) Percentage of service level agreements breached
2. Performance metrics for incident management
   (a) Volume of incidents detected and responded via automation
   (b) Dwell time (i.e. the duration a threat actor has undetected access until completely removed)
   (c) Recovery Point objectives (RPO) and recovery time objectives (RTO) satisfied

Recovery

RM-9.1.46 **Licensees must identify the critical systems and services within its operating environment that must be recovered on a priority basis in order to provide certain minimum level of services during the downtime and determine how much time the licensee will require to return to full service and operations.**

RM-9.1.47 Critical incidents are defined as incidents that trigger the BCP and the crisis management plan. Critical systems and services are those whose failure can have material impact on any of the following elements:

a) Financial situation;
b) Reputation;
c) Regulatory, legal and contractual obligations; and
d) Operational aspects and delivery of key products and services.

RM-9.1.48 **Licensees must define a program for recovery activities for timely restoration of any capabilities or services that were impaired due to a cyber security incident. Licensees must establish recovery time objectives ("RTOs"), i.e. the time in which the intended process is to be covered, and recovery point objectives ("RPOs"), i.e. point to which information used must be restored to enable the activity to operate on resumption". Licensees must also consider the need for communication with third party service providers, customers and other relevant external stakeholders as may be necessary.**

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.49 **Licensees must ensure that all critical systems are able to recover from a cyber security breach within the licensee's defined RTO in order to provide important services or some level of minimum services for a temporary period of time.**

RM-9.1.50 Licensees should validate that recovered assets are free of compromise, fully functional and meet the security requirements before returning the systems to normal business operations. This includes performing checks on data to ensure data integrity. In some cases, licensees may need to use backup data kept in a disaster recovery site or plan for the reconstruction of data from external stakeholders such as business partners and customers.

RM-9.1.51 **Licensees must define a program for exercising the various response mechanisms, taking into account the various types of exercises such as attack simulations, "war games" and "table top" exercises, and with reference to the relevant stakeholders such as technical staff, crisis management team, decision-makers and spokespersons.**

RM-9.1.52 **Licensees must define the mechanisms for ensuring accurate, timely and actionable communication of cyber incident response and recovery activities with the internal stakeholders, including to the board or designated committee of the board.**

RM-9.1.53 **Licensee must ensure its business continuity plan is comprehensive and includes a recovery plan for its systems, operations and services arising from a cyber security incident.**

RM-9.1 Cyber Security Risk Management (continued)

Cyber Security Insurance

RM-9.1.54 Licensees must arrange to seek cyber risk insurance cover from a suitable insurer, following a risk-based assessment of cyber security risk is undertaken by the respective licensee and independently verified by the insurance company. 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.

Training and Awareness

RM-9.1.55 Licensees must evaluate improvement in the level of awareness and preparedness to deal with cyber security risk to ensure the effectiveness of the training programmes implemented.

RM-9.1.56 The licensee 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. Additional training should be provided to 'higher risk staff'.

RM-9.1.57 The licensees must ensure that role specific cyber security training is provided on a regular basis to relevant staff including:

(a) Executive board and senior management;

(b) Cyber security roles;

(c) IT staff; and

(d) Any high-risk staff as determined by the licensee.

Reporting to CBB

RM-9.1.58 **Upon occurrence or detection of any cyber security incident, whether internal or external, that compromises customer information or disrupts critical services that affect operations, licensees must contact the CBB, immediately (within one hour), on 17547477 and submit Section A of the Cyber Security Incident Report (Appendix RM-1) to CBB's cyber incident reporting email, incident.investment@cbb.gov.bh, within two hours.**

RM-9.1.59 **Following the submission referred to in Paragraph RM-9.1.58, the licensee must submit to CBB Section B of the Cyber Security Incident Report (Appendix RM-1) within 10 calendar days of the occurrence of the cyber security incident. Licensees must include all relevant details in the report, including the full root cause analysis of the cyber security incident, its impact on the business operations and customers, and all measures taken by the licensee to stop the attack, mitigate its impact and to ensure that similar events do not recur. In addition, a weekly progress update must be submitted to CBB until the incident is fully resolved.**

RM-9.1.60 With regards to the submission requirement mentioned in Paragraph RM-9.1.58, the licensee should submit the report with as much information as possible even if all the details have not been obtained yet.

RM-9.1.61 **The penetration testing report as per Paragraph RM-9.1.29, along with the steps taken to mitigate the risks must be maintained by the licensee for a five-year period from the date of the report.**

Appendix A – Cyber Security Control Guidelines

The Control Guidelines consists of five Core tasks which are defined below. These Functions are not intended to form a serial path or lead to a static desired end state. Rather, the Functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cyber security risk.

Identify – Develop an organisation-wide understanding to manage cyber security risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Cyber Security Risk Management Framework. Understanding the business context, the resources that support critical functions, and the related cyber security risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Protect – Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cyber security incident.

Detect – Develop and implement appropriate activities to identify the occurrence of a cyber security incident. The Detect Function enables timely discovery of cyber security events.

Respond – Develop and implement appropriate activities to take action regarding a detected cyber security incident. The Respond Function supports the ability to contain the impact of a potential cyber security incident.

Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cyber security incident.

Below is a listing of the specific cyber security activities that are common across all critical infrastructure sectors:

IDENTIFY

Asset Management: The data, personnel, devices, systems, and facilities that enable the licensee to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the licensee's risk strategy.

1. Physical devices and systems within the licensee are inventoried.
2. Software platforms and applications within the licensee are inventoried.
3. Communication and data flows are mapped.
4. External information systems are catalogued.
5. Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
6. Cyber security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.

Business Environment: The licensee's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cyber security roles, responsibilities, and risk management decisions.

1. Priorities for the licensee's mission, objectives, and activities are established and communicated.
2. Dependencies and critical functions for delivery of critical services are established.
3. Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).

Governance: The policies, procedures, and processes to manage and monitor the licensee's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber security risk.

1. licensee's cyber security policy is established and communicated.
2. Cyber security roles and responsibilities are coordinated and aligned with internal roles and external partners.
3. Legal and regulatory requirements regarding cyber security, including privacy and civil liberties obligations, are understood and managed.
4. Governance and risk management processes address cyber security risks.

Risk Assessment: The licensee understands the cyber security risk to licensee's operations (including mission, functions, image, or reputation), licensee's assets, and individuals.

1. Asset vulnerabilities are identified and documented.
2. Cyber threat intelligence is received from information sharing forums and sources.
3. Threats, both internal and external, are identified and documented.
4. Potential business impacts and likelihoods are identified.
5. Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
6. Risk responses are identified and prioritized.

Risk Management Strategy: The licensee's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

1. Risk management processes are established, managed, and agreed to by licensee's stakeholders.
2. The licensee's risk tolerance is determined and clearly expressed.
3. The licensee's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.

Third Party Risk Management: The licensee's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing third party risk. The licensee has established and implemented the processes to identify, assess and manage supply chain risks.

1. Cyber third-party risk management processes are identified, established, assessed, managed, and agreed to by the licensee's stakeholders.

2. Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber third-party risk assessment process.
3. Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of a licensee's cyber security program.
4. Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
5. Response and recovery planning and testing are conducted with suppliers and third-party providers.

PROTECT

Identity Management, Authentication and Access Control: Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

1. Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
2. Physical access to assets is managed and protected.
3. Remote access is managed.
4. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
5. Network integrity is protected (e.g., network segregation, network segmentation).
6. Identities are proofed and bound to credentials and asserted in interactions
7. Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

Awareness and Training: The licensee's personnel and partners are provided cyber security awareness education and are trained to perform their cyber security-related duties and responsibilities consistent with related policies, procedures, and agreements.

1. All users are informed and trained on a regular basis.
2. Licensee's security awareness programs are updated at least annually to address new technologies, threats, standards, and business requirements.
3. Privileged users understand their roles and responsibilities.
4. Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.
5. The Board and senior management understand their roles and responsibilities.
6. Physical and cyber security personnel understand their roles and responsibilities.
7. Software development personnel receive training in writing secure code for their specific development environment and responsibilities.

Data Security: Information and records (data) are managed consistent with the licensee's risk strategy to protect the confidentiality, integrity, and availability of information.

Data-at-rest classified as critical or confidential is protected through strong encryption.

1. Data-in-transit classified as critical or confidential is protected through strong encryption.
2. Assets are formally managed throughout removal, transfers, and disposition
3. Adequate capacity to ensure availability is maintained.
4. Protections against data leaks are implemented.
5. Integrity checking mechanisms are used to verify software, firmware, and information integrity.
6. The development and testing environment(s) are separate from the production environment.
7. Integrity checking mechanisms are used to verify hardware integrity.

Information Protection Processes and Procedures: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational units), processes, and procedures are maintained and used to manage protection of information systems and assets.

1. A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).
2. A System Development Life Cycle to manage systems is implemented
3. Configuration change control processes are in place.
4. Backups of information are conducted, maintained, and tested.
5. Policy and regulations regarding the physical operating environment for licensee's assets are met.
6. Data is destroyed according to policy.
7. Protection processes are improved.
8. Effectiveness of protection technologies is shared.
9. Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
10. Response and recovery plans are tested.
11. Cyber security is included in human resources practices (e.g., deprovisioning, personnel screening).
12. A vulnerability management plan is developed and implemented.

Maintenance: Maintenance and repairs of information system components are performed consistent with policies and procedures.

1. Maintenance and repair of licensee's assets are performed and logged, with approved and controlled tools.
2. Remote maintenance of licensee's assets is approved, logged, and performed in a manner that prevents unauthorized access.

Protective Technology: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

1. Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
2. Removable media is protected and its use restricted according to policy.

3. The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
4. Communications and control networks are protected.
5. Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

DETECT

Anomalies and Events: Anomalous activity is detected and the potential impact of events is understood.

1. A baseline of network operations and expected data flows for users and systems is established and managed.
2. Detected events are analyzed to understand attack targets and methods.
3. Event data are collected and correlated from multiple sources and sensors
4. Impact of events is determined.
5. Incident alert thresholds are established.

Security Continuous Monitoring: The information system and assets are monitored to identify cyber security events and verify the effectiveness of protective measures.

1. The network is monitored to detect potential cyber security events.
2. The physical environment is monitored to detect potential cyber security events
3. Personnel activity is monitored to detect potential cyber security events.
4. Malicious code is detected.
5. Unauthorized mobile code is detected.
6. External service provider activity is monitored to detect potential cyber security events.
7. Monitoring for unauthorized personnel, connections, devices, and software is performed.
8. Vulnerability scans are performed at least quarterly.

Detection Processes: Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

1. Roles and responsibilities for detection are well defined to ensure accountability.
2. Detection activities comply with all applicable requirements.
3. Detection processes are tested.
4. Event detection information is communicated.
5. Detection processes are continuously improved.

RESPOND

Response Planning: Response processes and procedures are executed and maintained, to ensure response to detected cyber security incidents. Response plan is executed during or after an incident.

Communications: Response activities are coordinated with internal and external stakeholders.

1. Personnel know their roles and order of operations when a response is needed.
2. Incidents are reported consistent with established criteria.
3. Information is shared consistent with response plans.
4. Coordination with internal and external stakeholders occurs consistent with response plans.
5. Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness.
6. Incident response exercises and scenarios across departments are conducted at least annually.

Analysis: Analysis is conducted to ensure effective response and support recovery activities.

1. Notifications from detection systems are investigated.
2. The impact of the incident is understood.
3. Forensics are performed.
4. Incidents are categorized consistent with response plans.
5. Processes are established to receive, analyze and respond to vulnerabilities disclosed to the licensee from internal and external sources (e.g. internal testing, security bulletins, or security researchers).

Mitigation: Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

1. Incidents are contained.
2. Incidents are mitigated.
3. Newly identified vulnerabilities are mitigated or documented as accepted risks.

Improvements: The response activities are improved by incorporating lessons learned from current and previous detection/response activities.

1. Response plans incorporate lessons learned.
2. Response strategies are updated.

RECOVER

Recovery Planning: Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cyber security incidents. Recovery plan is executed during or after a cyber security incident.

Improvements: Recovery planning and processes are improved by incorporating lessons learned into future activities.

1. Recovery plans incorporate lessons learned.
2. Recovery strategies are updated.
3.

Communications: Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

1. Public relations are managed.
2. Reputation is repaired after an incident.
3. Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.