RISK MANAGEMENT MODULE

Table of Contents

RM-A.1 Purpose

Executive Summary

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

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

Legal Basis

RM-A.1.3 This Module contains the Central Bank of Bahrain's ('CBB') Directive (as amended from time to time) relating to risk management and is issued under the powers available to the CBB under Article 38 of the Central Bank of Bahrain and Financial Institutions Law 2006 ('CBB Law'). The Directive in this Module is applicable to insurance licensees (including their approved persons).

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

RM-A.2 Module History

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

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

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

Module Ref.	Change Date	Description of Changes
RM-1.1	01/07/05	Correction to cross-reference
RM-6.1	01/07/05	Clarified wording of factors to consider for operational risks.
RM-2.1	01/10/05	Clarified that the 25% notification for reinsurance exposure is to be applied based on a premium basis
RM-8.1	01/10/05	Corrected cross reference to in RM-8.1.6
RM-1.1	01/01/06	Clarified CBB's requirements for insurance firms to carry out their own assessment of their capital needs.
RM-2.1	01/01/06	Corrected cross-reference.
RM-6.1	01/07/06	Added requirements for physical security measures and third-party insurance to be put in place by insurance firms.
RM-A.1.3	01/2007	New Rule introduced, categorising this Module as a Directive.
RM-7.5.3	04/2008	Clarified that CBB prior approval is required for intra-group outsourcing
RM-7.2.1, 7.2.2 and 7.3.6	07/2008	Clarified that CBB prior approval is required for outsourcing arrangements
RM-7.5.7	04/2010	Added a Paragraph dealing with restrictions on intra-group outsourcing.
RM-A.1.3	01/2011	Clarified legal basis
RM-7.6	04/2013	Section amended on outsourcing of internal audit.
RM-1.1	04/2014	Enhanced the requirements for the risk management function.
RM-7.1.3	10/2017	Amended Paragraph to allow the utilization of cloud services.
RM-7.1.5A	10/2017	Added a new Paragraph on outsourcing requirements.
RM-7.2.1	10/2017	Amended Paragraph.
RM-7.2.3	10/2017	Amended Paragraph.
RM-7.2.6	10/2017	Amended Paragraph.
RM-7.2.8	10/2017	Added a new Paragraph on outsourcing.
RM-7.3.1	10/2017	Amended Paragraph.
RM-7.3.2	10/2017	Amended Paragraph.
RM-7.3.3	10/2017	Amended Paragraph.
RM-7.3.6	10/2017	Amended Paragraph.
RM-7.4.6	10/2017	Amended Paragraph.
RM-7.4.13	10/2017	Amended Paragraph.
RM-7.4.14	10/2017	Amended Paragraph.
RM-7.4.20	10/2017	Amended Paragraph.
RM-7.4.21	10/2017	Added a new Paragraph on security measures related to cloud services.
RM-7.5.3	10/2017	Amended Paragraph.
RM-7.5.4	10/2017	Amended Paragraph.
RM-9	10/2019	Added a new Section on Cyber Security.
RM-9	01/2022	New revised Chapter on Cyber Security Risk Management.
RM-9.1.58	04/2022	Amended Paragraph on cyber security reporting.
RM-9.1.59	04/2022	Amended Paragraph on the submission of the cyber security report.

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

RM-B.1 Scope

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

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

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

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

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

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

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

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

RM-1.1 Risk Management Systems and Controls

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

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

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

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

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

Risk Management

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

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

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

RM-1.1 Risk Management Systems and Controls (continued)

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

Risk Management Function

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

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

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

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

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

RM-2.1 Credit Risk

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

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

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

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

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

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

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

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

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

RM-2.1 Credit Risk (continued)

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

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

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

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

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

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

RM-3.1 Liquidity Risk

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

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

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

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

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

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

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

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

RM-4.1 Market Risk

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

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

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

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

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

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

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

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

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

RM-5.1 Insurance Technical Risk

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

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

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

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

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

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

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

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

RM-5.1 Insurance Technical Risk (continued)

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

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

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

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

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

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

RM-5.1 Insurance Technical Risk (continued)

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

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

(a) The adequacy and uncertainty of the technical claims provisions, such as outstanding claims, IBNR and claims handling expense reserves;

(b) The adequacy of other underwriting provisions, such as the provisions for unearned premium and unexpired risk reserves;

(c) The appropriateness of catastrophe models and underlying assumptions used, such as possible maximum loss (PML) factors used; and

(d) The effects of inflation.

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

RM-6.1 Operational Risk

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

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

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

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

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

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

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

RM-6.1 Operational Risk (continued)

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

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

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

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

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

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

Physical Security Measures

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

RM-6.1 Operational Risk (continued)

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

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

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

Third Party Insurance

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

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

RM-7.1 Introduction

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

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

RM-7.1.3 Outsourcing means an arrangement whereby a third party performs on behalf of a licensee an activity that was previously undertaken by the licensee itself (or in the case of a new activity, one which ordinarily would have been performed internally by the licensee). Examples of services that are typically outsourced include data processing, cloud services, customer call centres and back-office related activities.

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

RM-7.1.5 For purposes of Paragraph RM-7.1.2, a contract is 'material' where, if it failed in any way, it would pose significant risks to the on-going operations of a licensee, its reputation and/or the quality of service provided to its customers. For instance, the outsourcing of all or a substantial part of functions such as customer sales and relationship management, settlements and processing, IT and data processing and financial control, would normally be considered 'material'. Management should carefully consider whether a proposed outsourcing arrangement falls under this Module's definition of 'material'. If in doubt, management should consult with the CBB.

RM-7.1.5A For outsourcing services that are not considered material outsourcing arrangements, licenses must submit a written notification to the CBB before committing to the new outsourcing arrangement.

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

RM-7.1.7 **Insurance licensees must retain ultimate responsibility for functions or activities that are outsourced. In particular, licensees must ensure that they continue to meet all their regulatory obligations with respect to outsourced activities.**

RM-7.2 Supervisory Approach

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

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

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

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

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

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

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

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

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

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

RM-7.2.8 The CBB reserves the right to require a licensee to terminate or make alternative outsourcing arrangements if, among other reasons, the confidentiality of its customer information was, or is likely to be, breached or the ability of the CBB to carry out its supervisory functions in view of the outsourcing arrangement cannot be assured or executed.

RM-7.3 Risk Assessment

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

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

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

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

RM-7.3.5 **Licensees must maintain and regularly review contingency plans to enable them to set up alternative arrangements – with minimum disruption to business – should the outsourcing contract be suddenly terminated or the outsourcing provider fail. This may involve the identification of alternative outsourcing providers or the provision of the service in-house. These plans should consider how long the transition would take and what interim arrangements would apply.**

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

RM-7.4 Outsourcing Agreement

RM-7.4.1 The activities to be outsourced and respective contractual liabilities and obligations of the outsourcing provider and licensee must be clearly specified in an outsourcing agreement. This agreement must – amongst other things – address the issues identified below in this Section.

Control Over Outsourced Activities

RM-7.4.2 The Board and management of licensees are held ultimately responsible by the CBB for the adequacy of systems and controls in outsourced activities. Licensees must therefore ensure they have adequate mechanisms for monitoring the performance of, and managing the relationship with, the outsourcing provider.

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

RM-7.4.4 Once an outsourcing agreement has been entered into, licensees must regularly review the suitability of the outsourcing provider and the on-going impact of the agreement on their risk profile and systems and controls framework. Mechanisms for the regular monitoring by licensees of performance against Service Level Agreement and other targets, and for implementing remedies in case of any shortfalls, must also form part of the agreement. Such reviews should take place at least every year.

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

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

RM-7.4 Outsourcing Agreement (continued)

Customer Data Confidentiality

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

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

RM-7.4.9 For purposes of Paragraph RM-7.4.8, the implementation of adequate safeguards and procedures would include the proper segregation of customer data from those belonging to other clients of the outsourcing provider. Outsourcing providers should give suitable undertakings that the company and its staff will comply with all applicable confidentiality rules. Licensees should have contractual rights to take action against the service provider in the event of a breach of confidentiality.

RM-7.4.10 **Licensees must ensure that they retain title under any outsourcing agreements for data, information and records that form part of the prudential records of the firm.**

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

Access to Information

RM-7.4.12 **Outsourcing agreements must ensure that the licensee's internal and external auditors have timely access to any relevant information they may require to fulfil their responsibilities. Such access must allow them to conduct on-site examinations of the outsourcing provider, if required.**

RM-7.4.13 **Licensees must also ensure that the CBB inspectors and appointed experts have timely access to any relevant information they may reasonably require to fulfil its responsibilities under the law. Such access must allow the CBB to conduct on-site examinations of the outsourcing provider, if required.**

RM-7.4 Outsourcing Agreement (Continued)

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

RM-7.4.15 The outsourcing provider must commit itself, in the outsourcing agreement, to informing the licensee of any developments that may have a material impact on its ability to meet its obligations. These may include, for example, relevant control weaknesses identified by the outsourcing provider's internal or external auditors, and material adverse developments in the financial performance of the outsourcing provider.

Business Continuity

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

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

Termination

RM-7.4.18 Licensees must have a right to terminate the agreement should the outsourcing provider:

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

RM-7.4.19 Termination under any other circumstances allowed under the agreement must give licensees a sufficient notice period in which they can effect a smooth transfer of the service to another provider or bring it back in-house.

RM-7.4 Outsourcing Agreement (Continued)

RM-7.4.20

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

Cloud services

RM-7.4.21

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

(a)Customer information must be encrypted and licensees must ensure that all encryption keys or similar forms of authentication are kept secure within the licensee's control;

(b) A secure audit trail must be maintained for all actions performed at the cloud services outsourcing provider;

(c)A comprehensive change management procedure must be developed to account for future changes to technology with adequate testing of such changes;

(d) The licensee's data must be logically segregated from other entities data at the outsourcing service provider's platform;

(e)The cloud service provider must provide information on measures taken at its platform to ensure adequate information security, data security and confidentiality, including but not limited to forms of protection available against unauthorized access and incident management process in cases of data breach or data loss; and

(f) The right to release customer information/data in case of foreign government/court orders must be the sole responsibility of the licensee, subject to the CBB Law.

RM-7.5 Intra-group Outsourcing

RM-7.5.1 **As with outsourcing to non-group companies, the Board and management of licensees are held ultimately responsible by the CBB for the adequacy of systems and controls in activities outsourced to group companies.**

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

RM-7.5.3 **A licensee must obtain CBB prior written approval before committing to a material intra-group outsourcing. The request for approval must be made in writing to the licensee's normal supervisory contact at least 6 weeks prior to committing to the outsourcing and must set out a summary of the proposed outsourcing, its rationale, and an analysis of its associated risks and proposed mitigating controls.**

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

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

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

RM-7.5.7 **Insurance licensees may not outsource their core business activities to their group. The outsourcing of certain functions is subject to the provisions of Modules RM (Risk Management), HC (High-Level Controls) and FC (Financial Crime).**

RM-7.6 Internal Audit

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

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

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

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

RM-7.6.5 **In all circumstances, Board and management of licensees must retain responsibility for ensuring that an adequate internal audit programme is implemented and will be held accountable in this respect by the CBB.**

RM-8.1 Group Risk

RM-8.1.1 **Section RM-8.1 applies only to <u>Bahraini insurance firms</u> and <u>Bahraini insurance brokers.</u>**

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

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

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

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

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

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

RM-8.1 Group Risk (continued)

RM-8.1.8

In assessing group systems and controls, an <u>insurance licensee</u> must give consideration to:

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

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

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

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

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

RM-9.1 Cyber Security Risk Management

Role of the Board and Senior Management

RM-9.1.1 **The Board of insurance 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 boards~~,~~ 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 **Insurance firms must establish a cyber security risk function, independent of the information technology (IT) department, which must report to an independent risk management function or an equivalent function within the licensee. The cyber security risk management function must monitor and report on the status and maturity of relevant cyber security controls. Other insurance 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 insurance 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) to 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. 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-9.1.25, 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 who are rotated out 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:

Executive board and senior management;
Cyber security roles;
IT staff; and
Any high-risk staff as determined by the licensee.

RM-9.1 Cyber Security Risk Management (continued)

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.insurance@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 and must be provided to CBB**

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.

1. Data-at-rest classified as critical or confidential is protected through strong encryption.
2. Data-in-transit classified as critical or confidential is protected through strong encryption.
3. Assets are formally managed throughout removal, transfers, and disposition
4. Adequate capacity to ensure availability is maintained.
5. Protections against data leaks are implemented.
6. Integrity checking mechanisms are used to verify software, firmware, and information integrity.
7. The development and testing environment(s) are separate from the production environment.
8. 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.

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.