RISK MANAGEMENT MODULE

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

RM-9.1 Cyber Security Risk Measures

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

Training

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

Role of Board and Senior Management

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

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

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

RM-9.1 Cyber Security Risk Measures (continued)

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

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

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

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

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

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

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

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

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

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

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

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

RM-9.1 Cyber Security Risk Measures (continued)

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

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

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

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

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

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

RM-9.1 Cyber Security Risk Measures (continued)

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

a) Crisis management expenses such as costs of notifying affected parties, costs of forensic investigation, costs incurred to determine the existence or cause of a breach, regulatory compliance costs, costs to analyse the insured's legal response obligations;
b) Claim expenses such as costs of defending lawsuits, judgments and settlements, and costs of responding to regulatory investigations;
c) Policy also provides coverage for a variety of torts, including invasion of privacy or copyright infringement. First-party coverages may include lost revenue due to interruption of data systems resulting from a cyber or denial of service attack and other costs associated with the loss of data collected by the insured.

Security Breach

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

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

RM-9.1 Cyber Security Risk Measures (continued)

Independent testing

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

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