BERMUDA MONETARY AUTHORITY

CONSULTATION PAPER

AMENDMENT TO THE GROUP SUPERVISION RULES

MAY 2021

TABLE OF CONTENTS

We invite stakeholders, others within the financial services industry and any other interested persons to share their views on the proposals set out in this paper. Comments should be sent to the Authority, addressed to policy@bma.bm not later than 11 June 2021.

I. Introduction

1. The Bermuda Monetary Authority (Authority or BMA) has recently undertaken to enhance its oversight of operational cyber risks as part of the ongoing development of Bermuda's regulatory framework by introducing a new Insurance Sector Operational Cyber Risk Management Code of Conduct (Cyber Code).

2. Accordingly, the Authority, in the exercise of the powers conferred by the Insurance Act 1978 section 27F, is proposing to amend the Insurance (Group Supervision) Rules 2011 (Rules) to bring them in line with the requirements of the new Cyber Code, give certain sections greater clarity and make other changes to facilitate more effective administration of the Rules. The BMA does not intend to oversee the cyber risk of insurance groups where the BMA is not the group supervisor.

3. The amendments to the Rules will cover, among other things, the following areas:

    (a) Adding new definitions
    (b) Clarifying certain corporate governance requirements
    (c) Adding to the risk management framework
    (d) Adding a new cyber reporting obligation

II. Proposed definition additions

4. In Part 1: Group Responsibilities and Governance, Interpretation, the Authority intends to add the following definitions:

    (a) "information asset" means any data, device or other components of the environment that supports information-related activities

    (b) "information security" means the preservation of an information asset's confidentiality, integrity and availability

    (c) "Chief Information Security Officer (CISO)" means the senior executive, by whatever title he/she is called, appointed by the registrant to oversee and implement its cyber risk programme and enforce its cyber risk policies

    (d) "cyber reporting event" means any act that results in unauthorised access to, disruption of or misuse of the electronic systems or information stored on such systems of an insurance group, including any breach of security leading to the loss, unlawful destruction or unauthorised disclosure of or access to such systems or information, where-

        (i) the event has the likelihood of adversely impacting policyholders or clients of members of the insurance group

(ii) a member of the insurance group has reached a view that there is a likelihood that loss of its system availability will have an adverse impact on its policyholders or clients

(iii) a member of the insurance group has reached a view that there is a likelihood that the integrity of its information or data has been compromised or that important information has been exfiltrated (stolen), which may have an adverse impact on its policyholders or clients

(iv) a member of the insurance group has become aware that there is a likelihood that there has been unauthorised access to its information systems whereby such would have an adverse impact on its policyholders or clients

(v) an event has occurred for which notice is required to be provided to a regulatory body or government agency by a member of the insurance group

(e) "cyber risk programme" means the insurance group's policies and procedures that establish and document the manner in which cyber risks are managed

III. Other proposed changes

5. In Part 1: Group Responsibilities and Governance, Corporate governance: general, section 4 (6) (a) and (b), the Authority intends to add a person responsible for information security (i.e. CISO) as a person to which senior executives and the parent board should have access.

   The CISO role must be allocated to an appropriately qualified member of staff or outsourced resource. It should be noted, however, that if the role is outsourced, oversight responsibility remains with the board. The role of the CISO is to deliver the cyber risk programme and is expected to be of sufficient seniority to facilitate the cyber risk programme's delivery.

6. In Part 1: Group Responsibilities and Governance, Corporate governance: responsibilities of the parent board, section 5 (7), the Authority intends to add the following:

   (f) a parent board is accountable for the insurance group's cyber risk posture and must ensure it provides overall strategic direction, adequate oversight and challenge to the group's information security, commensurate with the size and extent of cyber threats to its information assets

The board of directors and senior management team must have oversight of cyber risks and must approve a cyber risk policy document at least annually. Regular updates detailing the overall cyber risk status must be made available to the board and senior management team.

7. In Part 1: Group Responsibilities and Governance, Risk management and internal controls framework: Operational risk component, section 16(1), the Authority intends to add the following:

    (e) risks to its information assets, including those managed by related parties and third parties.

8. In Part 2: General provisions to ensure compliance, Designated insurer to report certain events, section 29, the Authority intends to add the following paragraphs (29A) and (29B):

    Cyber risk programme

    29A (1) Every insurance group shall implement a cyber risk programme to ensure the information security of its information assets.

    (2) The cyber risk programme shall be evidenced by such policies and documentation as the insurance group deems appropriate and shall reflect the nature, scale and complexity of the group's business, systems and operations.

    Cyber event reporting

    29B (1) Every insurance group that comes into the knowledge of, or where it has reason to believe that, a cyber reporting event resulting in significant adverse impact to the group's operations, policyholders or clients has occurred, shall within 72 hours from the time that there is either a determination or a confirmation of an event (whichever is sooner), notify the Authority in such manner as the Authority may direct.

    (2) Within 14 days of such notification, the insurance group shall furnish the Authority with a report in writing, setting out all the known pertinent particulars of the case that are available to it. If the root cause has not been confirmed, then the report must still be submitted detailing information known to date.

    (3) If the report in (2) does not include all the details due to event complexity and ongoing investigation, a full report containing root cause analysis should be submitted promptly once it is concluded.

9. The Authority will allow flexibility as to how the above cyber event reporting requirements will be met to absolve insurance groups of multiple reporting requirements and to promote efficiency:

    (a) Where the incident occurs in a jurisdiction where there is a similar reporting requirement at the local level, besides the notification of the incident (as proposed in 29B (1) above), the designated insurer shall also directly furnish to the Authority a copy of the written report that the insurance group member has submitted to the local regulator.

    As an alternative, the designated insurer may notify the Authority that such a written report has been submitted to the local regulator and the Authority, in its capacity as the group supervisor, will obtain the report or its particulars as part of college exchange of information agreement.

    (b) Bermuda legal entity incidents will be reported once—at the legal entity level and in line with the requirements of the Cyber Code

10. For the sake of clarity, the designated insurer is responsible for notifying the Authority of the reportable cyber event. When in doubt about whether an event is reportable, the designated insurer should consult with the Authority for guidance.

11. The Authority may request further updates where not all pertinent particulars of the reportable event are included in the report being filed or where sufficient information was not gathered as part of the college exchange of information.

12. Insurance groups are expected to keep the Authority regularly updated on progress through the remediation of the incident and related corrective actions.

***

BERMUDA

INSURANCE (GROUP SUPERVISION) AMENDMENT RULES 2021

BR /2021

The Bermuda Monetary Authority, in exercise of the powers conferred by section 27F of the Insurance Act 1978, makes the following Rules:

Citation

1 These Rules, which amend the Insurance (Group Supervision) Rules 2011 (principal Rules) may be cited as the Insurance (Group Supervision) Amendment Rules 2020.

Amends paragraph 2

2 Paragraph 4 of the principal Rules is amended by inserting the following definitions in their alphabetical order—

"information asset" means any data, device or other component of the environment that supports information-related activities;

"information security" means the preservation of an information asset's confidentiality, integrity and availability;

"cyber risk programme" means the policies and procedures of the insurance group that establish and document the manner in which cyber risk is managed;

"cyber reporting event" means any act that results in unauthorised access to, disruption of or misuse of the electronic systems or information stored on such systems of an insurance group, including any breach of security leading to the loss, unlawful destruction or unauthorised disclosure of or access to such systems or information, where-

(a) the event has the likelihood of adversely impacting policyholders or clients of members of the insurance group;

(b) a member of the insurance group has reached a view that there is a likelihood that loss of its system availability will have an adverse impact on its policyholders or clients;

(c) a member of the insurance group has reached a view that there is a likelihood that the integrity of its information or data has been compromised or that important information has been exfiltrated (stolen), which may have an adverse impact on its policyholders or clients;

(d) a member of the insurance group has become aware that there is a likelihood that there has been unauthorised access to its information systems whereby such would have an adverse impact on its policyholders or clients; or

(e) an event has occurred for which notice is required to be provided to a regulatory body or government agency by a member of the insurance group.

"Chief Information Security Officer (CISO)" means the senior executive, by whatever title he/she is called, appointed by the registrant to oversee and implement its cyber risk programme and enforce its cyber risk policies.

DRAFT

Amends paragraph 4

3 Paragraph 4 (6) of the principal Rules is amended—

(a) in subparagraph (a) by inserting after "audit," the words "cyber risk management programme,";

(b) in subparagraph (b) by inserting after "executives" the words "cyber information security officer".

Amends paragraph 5

4 Paragraph 5 (7) is amended by inserting the following new subparagraph after subparagraph "(e)" —

"(f) the group's cyber risk posture and must ensure it provides overall strategic direction, adequate oversight and challenge to the group's information security, commensurate with the size and extent of cyber threats to its information assets.

Amends paragraph 16

5 Paragraph 16 is amended by inserting the following new subparagraph after subparagraph "(d)"—

"(e) risks to its information assets including those managed by related parties and third parties."

Inserts paragraph 29A

6 The principals' Rules are amended by inserting the following new paragraph after paragraph 29—

Cyber risk programme

29A (1) Every insurance group shall implement a cyber risk programme to ensure the information security of its information assets.

(2) The cyber risk programme shall be evidenced by such policies and documentation as the insurance group deems appropriate, and shall reflect the nature, scale and complexity of the group's business, systems and operations.

Cyber event reporting

29B (1) Every insurance group that comes into the knowledge of, or where it has reason to believe that, a cyber reporting event resulting in significant adverse impact to the insurance group's operations, policyholders or clients has occurred, shall within 72 hours from the time that there is either a determination or a confirmation of an event (whichever is sooner) of such event, notify the Authority in such manner as the Authority may direct.

(2) Within 14 days of such notification, the insurance group shall furnish the Authority with a report in writing, setting out all the known pertinent particulars of the case that are available to it. If the root cause has not been confirmed, then the report must still be submitted detailing information known to date.

(3) If the report in (2) does not include all the details due to event complexity and ongoing investigation, a full report containing root cause analysis should be submitted promptly once it is concluded.

(4)(a) The report shall either be submitted by the designated insurer to the Authority or, where similar reporting requirements have been completed at local jurisdiction level for a member of the group, a copy of such report shall be furnished to the Authority.

(b) Where a notification is made to the Authority, but a copy of the local jurisdiction report referred to above is not furnished to the Authority, the Authority in its capacity as the group supervisor will seek to engage with and obtain the report or its particulars from the local jurisdiction regulator as part of supervisory college exchange of information.

DRAFT

Commencement

7 These Rules come into operation on July 1, 2022.

Made this day of 2021

Jeremy Cox
Executive Chairman
Bermuda Monetary Authority