Guidelines on Information and Cyber Security extended to Insurance Intermediary

October 11, 2022

Background

- IRDA initially had provided 'Guidelines on Information and Cyber Security for insurers' ('the guidelines') vide notification dated April 07, 2017
- Further, vide circular dated September 02, 2022, IRDA with immediate effect has extended the applicability of the guidelines to all insurance intermediaries covering **Brokers, Corporate Agents, Web Aggregators, Corporate Surveyors, Insurance Self Networking Platform (ISNP), and Insurance Repositories**.

The present circular dated October 11, 2022 has been issued to provide for the timeline for implementation of requirements in the said Guidelines

Sr No	Directions under revised IRDAI Cyber Security Guidelines	Timeline for implementation	IT Framework for NBFCs *(applicable to NBFCs & HFCs with asset size above ₹ 500 crore)*
1	Appointment of Chief Information Security Officer (CISO) responsible for enforcing the Cyber Security Policies.	31st Dec, 2022	No specific provision
2	Preparation of GAP Analysis Report as per Checklist	31st Dec, 2022	Required under para 6.4
3	Formulation of Cyber Crisis Management Plan	15th Jan, 2023	Required under para 3.5
4	Preparing Information and Cyber Security Policy, to be approved by Board of the Intermediary.	31st Jan, 2023	Required under para 3.1 and 3.2
5	Completion of Cyber Security Assurance Audit	28th Feb, 2023	Information Systems Audit required under para 5
6	Cyber Security Assurance Program (to close Gaps) as per Cyber Security Assurance Audit	31st Mar, 2023	As per para 5, NBFC's management is responsible to take actions on observations. But no specific mention of a 'Cyber Security Assurance Program'.

Auditor's Certificate:

Timeline: The intermediaries, after adhering to the above timelines, are required to file the Audit Report on or before March 31, 2023.

Format: Provided in the zip file

Eligibility: Audit firm to meet the following criteria:

a. Partnership Firm or LLP registered with ICAI;

b. Continuous 5 years of practice;

c. Minimum 5 partners, before the date on appointment where at least one partner-

   a. Is CISA/DISA of ICAI
   b. Is Fellow member of ICAI.
   c. Has a minimum 3 years of experience Cyber Security / Information Security review or Cyber Security / Information Security audit of either Insurance Companies or Banks or Mutual Funds.
   d. Has experience of certification of IRDAI's Investment Systems and Process of Insurance Companies.
   e. Has the experience of audit in IT environment and in conducting Audit from remote location.

Actionable:

- **For Insurance Intermediaries – To implement the guidelines in totality**
- **For Financial sector entities that are registered as Corporate Agents**
  - Several requirements are already applicable. Refer Annexure 1.
  - Gap analysis to be done in terms of the additional requirements under the Guidelines.
  - Eligibility of the existing IS Auditor to be ascertained in terms of these Guidelines.

Vinod Kothari & Company
Mumbai| Delhi | Kolkata
corplaw@vinodkothari.com

Guidelines on Information and Cyber Security extended to Insurance Intermediary

October 11, 2022

Annexure 1

Sr. no.	Directions under revised IRDAI Cyber Security Guidelines	Timeline for implementation	Related provision under the IT Framework for NBFCs (applicable to NBFCs & HFCs with asset size above Rs.500 crore)	Related provision for Scheduled Commercial Banks under the Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds
1	Appointment of Chief Information Security Officer (CISO) responsible for enforcing the Cyber Security Policies.	31st Dec, 2022	As per para 2.b, designate a senior executive as a Chief Information Officer to ensure implementation of IT Policy to the operational level involving IT strategy, value delivery, risk management and IT resource management	A sufficiently senior level official, of the rank of GM/DGM/AGM, should be designated as Chief Information Security Officer pursuant to Chapter 2
2	Preparation of GAP Analysis Report as per Checklist	31st Dec, 2022	As para 6.4, the GAP Analysis along with Board's insight should form the basis for construction of the Business Continuity Policy.	Gap analysis forms part of the Information Security (IS) Assessment.
3	Formulation of Cyber Crisis Management Plan	15th Jan, 2023	Under para 3.5, Cyber Crisis Management Plan should be a part of the overall Board approved strategy.	Required to have in place a crisis management program along with a Crisis Management Team.
4	Preparing Information and Cyber Security Policy, to be approved by Board of the Intermediary.	31st Jan, 2023	Under para 3.1 and 3.2, Board-approved Information Security Policy and Cyber Security Policy are required to be put in place by the Company.	Required to have in place a cyber security policy which is evaluated under the IS Assessment
5	Completion of Cyber Security Assurance Audit	28th Feb, 2023	As para 5, Information Systems Audit should be conducted at least once in a year.	Information security assurance includes penetration testing, IS Audits, IS Assessments. Additionally, upon reporting of IS Audit findings, periodical follow-ups and review of Action Taken Report shall be carried out by the IS Auditor
6	Cyber Security Assurance Program (to close Gaps) as per Cyber Security Assurance Audit	31st Mar, 2023	As per para 5, NBFC's management is responsible to take actions on observations. But there is no specific mention of a 'Cyber Security Assurance Program'.	

Vinod Kothari & Company
Mumbai| Delhi | Kolkata
corplaw@vinodkothari.com