

Annexure A: Amendments to IRDAI Cybersecurity Guidelines, 2023 and Security Controls

A. Guidelines

S.N	Existing Guidelines	Revised Guidelines	Para/ Clause No.
1	Applicability- FRBs New Provision for compliance by FRBs	a. As long as governance responsibilities outlined in the specified committees are met at regional / controlling / head office for complying with these guidelines, they may not constitute committees at the branch level. b. W.r.t to compliance with the provisions of guidelines or controls provided in the checklist (annexure-III), FRBs shall 'comply or explain', subject to a reasonably justifiable explanation, as a part of the supervisory process.	1.4 Applicability- FRBs
2	ISPMC shall meet at least twice in a year.	The Information Security Risk Management Committee (ISPMC) shall meet at least on a quarterly basis.	1.5 (II) Governing Board
3	Board of Directors New provisions (additional responsibilities)	a. Provide sufficient budget for Information and Cyber security keeping in view the current/emerging threat landscape and ensure that the budget is proportional to the organization's risk appetite. b. Receive the status of non-conformities observed in the annual cyber security assurance audit report and risk report. c. Approve timelines for closure of gaps observed and ensure that gaps are closed within 12 months of reporting.	1.6 (1) Roles and Responsibilities - Board of Directors
4	a. Briefing to the ISPMC b. CISO shall review and approve requested	a. The CISO shall not have direct reporting relationship with the Head of IT Function and shall not be given any business targets. The CISO	1.6 (3) Roles and Responsibilities – Chief

	<p>exceptions to information security policies, standards and procedures</p> <p>The above provisions are modified and new additional responsibilities are prescribed.</p>	<p>should be adequately staffed with people having relevant technical expertise.</p> <p>b. Briefing to the ISRMC and the Board.</p> <p>c. Shall be Permanent invitee to IT Steering Committee.</p> <p>d. The CISO shall review and comment on each of requested exceptions to information security policies, standards and procedures.</p> <p>e. The CISO shall develop and implement Scenario based Incident Response plans to deal with Cyber crises, contingencies and disasters, attacks on IT systems etc.</p> <p>f. The CISO shall be responsible for complying with guidelines issued by Cert-In from time to time.</p>	Information Security Officer (CISO)
5	CTO shall be responsible for the information security related technology implementation of the organization.	<p>Chief Technology Officer(CTO) /Head of IT Function:</p> <p>a. CTO shall enable and support implementation of the security related technology and processes within the organization in consultation or agreement with CISO.</p> <p>b. CTO shall ensure that information technology and processes are in line with the IS standards defined by the CISO.</p> <p>c. CTO shall ensure that all identified vulnerabilities through internal/external audits or Risk Assessment are remediated in a timely manner.</p>	1.6 (4) Roles and Responsibilities – Chief Technology Officer(CTO)
6	CITSO Detailed Roles and Responsibilities	The requirement of having a CITSO designation has been removed. However, organizations to ensure all functions envisaged to be done by the	1.6 (5) Roles and Responsibilities – Chief IT

		erstwhile CITSO are under the job definitions of CISO/CTO as may be applicable.	Security Officer (CITSO)
7	Chief Security Officer (CSO) / Admin / Head Administration Detailed Roles and Responsibilities	The roles and responsibilities prescribed in the guidelines are baseline governance controls, however, REs may adopt enhanced controls commensurate with their risk profile, size, and complexity.	1.6 (6) Roles and Responsibilities –Chief Security Officer (CSO) / Admin / Head Administration
8	Functional Head/ Business Owner New provision (additional responsibilities)	<p>a. Ensure the implementation and adherence to cybersecurity policies, procedures, and guidelines by all team members.</p> <p>b. Collaborate with the organization's Chief Information Security Officer (CISO) to assess and address specific cybersecurity risks associated with the business unit/function.</p> <p>c. Report and escalate cybersecurity incidents promptly to the designated incident response team.</p>	1.6 (12) Roles and Responsibilities – Functional Head/ Business Owner
9	ISRMC shall provide relevant periodic assurances to the Control Management Committee (CMC)	<p>a. The ISRMC shall report the status of non-conformities observed in the annual cyber security assurance audit report along with timelines for closure of gaps observed, to the RMC, which in turn will take to the Board serious non-conformities, if any, observed.</p> <p>b. The Committee shall provide relevant periodic assurances to the Risk Management Committee (RMC) on a quarterly basis.</p>	1.6 (13) Roles and Responsibilities –Information Security Risk Management Committee (ISRMC)
10	New Provision IT Steering Committee (ITSC)	<p>a. The Organization shall establish a IT Steering Committee with representation at senior management level from IT and Business functions.</p> <p>b. Assist the Board in developing the IT strategy for the Organization in alignment with business needs.</p>	1.6 (14) Roles and Responsibilities –IT Steering Committee (ITSC)

		<p>c. Ensure implementation of a robust IT architecture meeting statutory and regulatory compliance.</p> <p>d. Ensuring all IT Related SLAs/SOWs are in alignment with regulatory requirements and periodic review of SLA monitoring process.</p> <p>e. Ensure effective implementation and governance of business continuity and disaster recovery frameworks.</p> <p>f. Monitor the effectiveness of controls established to protect policyholder data within IT systems.</p> <p>g. On Aspects of IT Procurements or projects, software license subscriptions, SaaS Service subscriptions, tools procurement etc. which have a bearing on Information Security, the Committee needs to obtain the inputs from CISO function to ensure IT and IT Security are aligned on such decisions.</p> <p>h. Update RMC & CEO periodically on activities of ITSC.</p> <p>i. The ITSC shall meet at least on a quarterly basis. The Chief Technological Officer shall be the convener of ITSC.</p>	
11	<p>Control Management Committee (CMC)</p> <p>Detailed Roles and Responsibilities</p>	The requirement of Control Management Committee (CMC), a board level committee, is done away with, however, Organizations are required to ensure that all functions envisaged to be done by the erstwhile CMC are part of Risk Management Committee (RMC) terms of reference.	1.6 (15) Roles and Responsibilities –Control Management Committee (CMC)
12	<p>Roles and Responsibilities</p> <p>New Provision</p>	Considering the importance of Cybersecurity in rapidly changing technological landscape, one or more Independent External Expert (IEE) having substantial IT and/or Cybersecurity expertise in	1.6 (16) Roles and Responsibilities- Independent

		managing or guiding IT/Cybersecurity related initiatives or projects, shall be a part of RMC.	External Expert (IEE)
13	Exceptions New Provision	<p>Exceptions not exceeding three months shall be approved by the Chief Information Security Officer (CISO) of the organisation. Exceptions exceeding three months shall be approved by the Risk Management Committee (RMC). Further, exceptions exceeding one year shall be approved by the Board of Directors of the organisation.</p> <p>Also, it is required that any exception request exceeding 12 months must undergo a reassessment and re-approval process.</p> <p>All exceptions granted should formally document risk associated with granting such exceptions.</p>	1.9 (II) Exceptions
14	<p>Compliance: The Insurance Intermediary shall submit the Annexure – III along with compliance thereto and the comments of the board to the Insurer/s annually.</p> <p>New Provision</p>	<p>a. The Insurance Intermediary shall submit the Annexure – III along with compliance thereto and the comments of the Audit Committee / Risk Management Committee / Board of Directors / Principal Officer, as applicable, to the Insurer/s annually, within 30 days of completion of Audit by a Cert-In Empaneled Auditor or Audit firm as prescribed under Annexure IV of the guidelines.</p> <p>b. Also, Regulated Entities must take appropriate technical and organizational measures to comply with the provisions of Digital Personal Data Protection Act (DPDP) and rules made thereunder.</p>	1.10 Compliance
15	<p>Security Domain</p> <p>Detailed description of Policies</p>	This section is a guidance document for Regulated Entities to frame their own policies, specifying appropriate and adequate security controls along with the applicable standards. The	2.0 - Security Domain Policies

		policies shall encompass each of the security domains provided and shall be a part of their approved Information and Cyber Security Policy.	
--	--	---	--

B. Auditors Report:

S.N	Existing	Revised Controls	Control No and Area
1	New Control	Group companies' infrastructure, networks, and databases are logically and/or physically segregated, and where a vendor provides services to group companies, IT personnel with cross-entity access are segregated, wherever possible	32 - Security Continuous Monitoring & Detection (DE.CM):
2	Is External Black box Penetration Testing (PT) conducted for all internet facing information assets or systems once in a 6 months	Is External Grey/White box Penetration Testing (PT) conducted for all internet facing information assets or systems at least once in 6 months by a CERT-In empaneled Auditor.	96- Security Continuous Monitoring & Detection (DE.CM):
3	New Control	Whether, in cases where PT is conducted in a test environment due to unavoidable circumstances, the organization ensures that the test environment's version and configuration resemble the production environment for VAPT, and any deviations are placed before the ISRMC for approval?	97- Security Continuous Monitoring & Detection (DE.CM):
4	New Control	Does the organization maintain an up-to-date inventory of its cryptographic assets to ensure preparedness for transition to post-quantum cryptographic environments?	110- Asset Management (ID.AM)
5	New Control	Whether the Regulated Entity, through SLAs, requires service providers/outsourced entities to obtain prior written permission before any further outsourcing	148 - Supply Chain Risk Management (ID.SC)

6	New Control	Is the Cloud Service Provider (CSP) MeitY empaneled CSP and holds a valid STQC (or any other equivalent agency appointed by Government of India) audit status?	149 - Supply Chain Risk Management (ID.SC)
7	New Control	Has the organization signed NDA with CSP covering all aspects relating to privacy, confidentiality, security and business continuity?	150-Supply Chain Risk Management (ID.SC)
8	New Control	Does the organization contractually require that the cloud service provider will completely eliminate any trace of data/ information in disks, backups, etc., at the termination of the contract?	151- Supply Chain Risk Management (ID.SC)
9	Is appropriate hardware backup available?	Is appropriate immutable backup and Failover/Resilient components available for critical hardware?	204- Information Protection Processes and Procedures (PR.IP):