Consultation Paper on Guidelines on Cyber Security and Cyber Resilience for the Market Infrastructure Institutions (MIIs) in IFSC

Objective

1. The objective of this consultation paper is to seek comments / views from Market Infrastructure Institutions (MIIs) and other relevant stakeholders on the draft "Guidelines on Cyber Security and Cyber Resilience for the Market Infrastructure Institutions (MIIs) in IFSC"

Background

2. IFSCA has issued the 'Guidelines on Cyber Security and Cyber Resilience for Regulated Entities in IFSCs' on March 10, 2025. These principle-based guidelines aim to provide a consistent, proportional and risk-based regulatory framework, based on global best practices, for the management of cyber risk in IFSC.

3. IFSCA, as a member of IOSCO, has adopted the Principles for Financial Market Infrastructures (PFMIs) laid down by CPMI-IOSCO.

4. Principle 17 of the PFMI relates to management and mitigation of 'Operational risk'. This principle requires systemically important market infrastructures institutions to

   "identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption."

   Cyber risk therefore forms a critical component of operational risk.

5. The MIIs provide the necessary infrastructure for listing, trading, clearing and settlement of securities and form the crucial pillars of the capital market ecosystem. At present, there are two Stock Exchanges, one Bullion exchange, two Clearing Corporations and one Depository operational in IFSC. There is a high degree of operational interconnectivity between these MIIs, associated

intermediaries and financial market participants. Any cyber incidents affecting these institutions can have far-reaching implications for financial stability and market integrity.

6. Given the potential systemic impact, a differentiated and elevated baseline of cyber security and cyber resilience is necessary for MIIs in IFSCs. Accordingly, the draft "***Guidelines on Cyber Security and Cyber Resilience for the Market Infrastructure Institutions (MIIs) in IFSC***" have been prepared and placed at **Annexure A**.

7. Comments are invited on the draft "***Guidelines on Cyber Security and Cyber Resilience for the Market Infrastructure Institutions (MIIs) in IFSC"***. The comments may be sent by an email to Shri Praveen Kamat, General Manager & CISO at praveen.kamat@ifsca.gov.in with a copy to cybersecurity.ifsc@ifsca.gov.in with the subject line ***"Comments on the Guidelines on Cyber Security and Cyber Resilience for the Market Infrastructure Institutions (MIIs) in IFSCs".***

The comments may be sent latest by December 16, 2025.

The comments should be provided in the following format:

Name and Designation				
Contact No. and Email Address				
Name of Organisation				
S. No.	**Para/clause no. of the master circular**	**Text of the clause**	**Comments/ Suggestions**	**Detailed Rationale**

Annexure A

Guidelines on Cyber Security and Cyber Resilience for Market Infrastructure Institutions (MIIs) in IFSC

Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases of financial institutions. Cyber security framework includes measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience. Cyber Resilience is an organisation's ability to prepare and respond to a cyber-attack and to continue operation during, and recover from, a cyber-attack.

I. Govern

1. The Market Infrastructure Institutions (MIIs), as part of their operational risk management framework, shall formulate a comprehensive Cyber Security and Cyber Resilience Policy ("Policy") to manage risks to their systems, networks, and databases posed by cyber-attacks and threats. This Policy document shall encompass the guidelines specified within this framework.

2. The Policy document must be approved by the Governing Board (Board) of the MIIs. In case of deviations from the suggested framework, reasons for the same shall also be provided in the Policy document. Furthermore, the Board shall review the Policy document at least annually to strengthen and improve the MII's cyber security and cyber resilience framework.

3. The MIIs shall prepare a risk appetite and risk tolerance statement as part of the Policy that articulates the nature and extent of cyber security risks that the MIIs are willing and able to assume. The Board and Senior Management shall ensure that key IT decisions are made in accordance with the MII's risk appetite and risk tolerance statement.

4. The Policy shall establish a structured framework to identify, assess, and manage cybersecurity risks associated with the organization's processes, information, networks, and systems. This framework shall comprise the following key processes:

    i. 'Identify' critical IT assets and risks associated with such assets.

ii. 'Protect' assets by deploying suitable controls, tools, and measures.

iii. 'Detect' incidents, anomalies, and attacks through appropriate monitoring tools/processes.

iv. 'Respond' by taking immediate steps after identification of the incident, anomaly, or attack.

v. 'Recover' from incident through incident management, disaster recovery, and business continuity framework.

5. The Policy shall undergo periodic review and updates to dynamically adapt to the emerging cyber threat landscape and incorporate advancements in cybersecurity technologies and practices, ensuring its ongoing effectiveness.

6. The Standing Committee on Technology (SCOT) of the MIIs shall review the implementation of the Policy on a biannual basis.

7. For MIIs that have been identified as Critical Infrastructure Institutions (CII) by National Critical Information Infrastructure Protection Centre (NCIIPC), the policy shall encompass the principles prescribed by NCIIPC of the National Technical Research Organisation (NTRO), Government of India in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time.

8. The MIIs shall appoint a dedicated Chief Information Security Officer (CISO) who will be responsible for:

   i. Assessing, identifying, and mitigating cybersecurity risks;
   ii. Responding to cybersecurity incidents;
   iii. Establishing cybersecurity standards and controls;
   iv. Implementing the necessary processes as per the Board-approved cybersecurity and resilience policy.

   The CISO shall report directly to the Managing Director (MD)/Chief Executive Officer (CEO).

9. For the MIIs designated as CII by NCIIPC, the CISO's roles and responsibilities shall also adhere to the aforesaid NCIIPC guidelines.

10. The Board and the Senior Management shall have members with the requisite knowledge to understand and manage risks posed by cyber threats.

11. The MIIs shall establish a reporting procedure to facilitate communication of unusual activities and events to CISO or to the Senior Management in a timely manner.

12. The MIIs shall define the responsibilities of their employees, outsourced staff, and employees of vendors, members or participants, and other entities, who may have access to or use systems/networks of MIIs, towards ensuring the goal of cyber security.

II. Identify

13. The MIIs shall maintain an up-to-date inventory of their (including but not limited to) hardware and systems, software, digital assets (such as URLs, domain names, applications, APIs, etc.), shared resources (including cloud assets), interfacing systems (internal and external), details of its network resources, connections to its network and data flows.

14. Any additions/ deletions or changes in existing assets shall be reflected in the asset inventory within 3 working days.

15. The MIIs shall identify and classify critical assets based on their sensitivity and criticality for business operations, services, and data management. The critical assets shall include business-critical systems, internet-facing applications /systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical assets, either for operations or maintenance, shall also be classified as critical assets. Further, The Board of the MIIs shall approve the list of critical assets.

16. The MIIs shall accordingly identify cyber security risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business, and thereby, deploy controls commensurate to the criticality.

17. The MIIs shall prepare and maintain an up-to-date network architecture diagram at the organizational level including wired and wireless networks.

18. The MIIs shall conduct a risk assessment (including post-quantum risks) of the IT environment of their organization on a half-yearly basis to acquire visibility and a reasonably accurate assessment of the overall cybersecurity risk posture.

III. Protect

Access Controls

19. No person by virtue of rank or position shall have any intrinsic right to access confidential data, applications, system resources, or facilities.

20. Access to all systems, applications, networks, databases, etc., shall be for a defined purpose and for a defined period. The MIIs shall grant access to their IT systems, applications, databases and networks on a need-to-use basis and on the principle of least privilege. Such access shall be authorized using strong authentication mechanisms and shall be immediately revoked upon expiration of the required period. Additionally, solutions like Privileged Identity Management (PIM)/ Privileged Access Management (PAM) shall be put in place.

21. The MIIs shall implement strong password controls for users' access to systems, applications, networks, and databases. Password controls shall include a change of password upon first log-on, minimum password length and history, password complexity as well as the maximum validity period. The user credential data shall be stored using secure cryptographic hashing algorithms.

22. The User access rights, delegated access unused tokens, and privileged user activities shall be reviewed on a quarterly basis.

23. The MIIs shall ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs shall be maintained and stored in a secure location for a period not less than two (2) years. The MIIs also need to maintain records of users with access to shared accounts.

24. All critical systems accessible over the internet shall have layered security (such as VPNs, Firewall controls, etc.) and Multi-Factor Authentication (MFA).

25. The MIIs shall deploy additional controls and security measures to supervise staff who have elevated system access (such as admin or privileged users) and access to critical assets. Such controls and measures shall inter-alia include:

    i. restricting the number of privileged users,
    ii. periodic review of privileged users' activities,
    iii. disallowing privileged users from accessing systems logs in which their activities are being captured,
    iv. strong controls over remote access by privileged users, etc.

26. The MIIs shall implement a robust dual authorization mechanism (maker-checker principle) for all access to critical information systems. The MII shall ensure that no single individual possesses unilateral authority to execute changes to access controls.

    The following controls shall be specifically adhered to:

    i. All access requests to critical systems shall require written or electronically documented approval from appropriately authorized personnel before implementation.

    ii. The Maker (the individual initiating the access request) and the Checker (the individual approving and implementing the access change) must be distinct individuals, with no subordinate-superior relationship between them.

    iii. All access modifications (including provisioning, modification, or revocation of access to critical systems) shall maintain a non-repudiable audit trail documenting the:

        a. identity of both the maker and checker,
        b. timestamp of the action, and
        c. business justification

27. The MIIs shall also enforce periodic rotation of personnel holding administrative or privileged access to critical systems at intervals not exceeding 12 months, or upon change of role/responsibilities, whichever is earlier.

28. The MIIs shall formulate an internet access policy to monitor and regulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc.

29. A proper 'end of life' protocol shall be adopted to deactivate access privileges of users:

    i. upon their cessation of employment or
    ii. upon formal withdrawal of access privileges

30. Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the MII's critical systems, networks, and other computer resources, shall be subject to stringent supervision, monitoring and access restrictions.

Security of Active Directory (AD) and Domain Controllers (DCs)

31. The MIIs shall regularly review the Active Directory (AD) to locate and close existing backdoors such as compromised service accounts, which often have administrative privileges and are a potential target for attacks.

32. As threat actors frequently leverage Domain Controllers (DCs) to launch network-wide malware attacks, the MIIs shall ensure immediate application of all released security patches to DCs. This patching requirement shall be subject to a quarterly review.

33. In order to minimize the attack surface, the MIIs shall ensure that software that is not essential to the core functioning of the DC is not installed on the DC.

34. All access to DCs shall be restricted to the Administrators group. Users within this group shall maintain separate, non-privileged user accounts for all day-to-day operational activities.

35. The MIIs shall ensure that the DC does not have direct internet access and that the connectivity to the DC adheres to the principle of least privilege. Any necessary external communication shall be strictly controlled and explicitly whitelisted through a secure firewall or proxy server.

36. The MIIs shall undertake the penetration testing activity (internal and external) for known Active Directory Domain Controller abuse attacks. Any weaknesses detected shall be remediated on a priority basis.

Insider Threat

37. Insider threat shall inter alia include acts such as:

    a. theft of confidential data,
    b. sabotage of IT systems, and
    c. fraud committed by the staff, including contractors or service providers

38. As the human element plays an important role in managing IT systems and processes in an IT environment, the MIIs shall ensure that all personnel, including contractors and service providers, have the requisite level of competence and skills to perform the IT functions and manage the cyber security risks.

Physical security

39. Physical access to the critical systems shall be restricted to a minimum. Physical access of outsourced staff/visitors shall be properly supervised by ensuring at the minimum that outsourced staff/visitors are always accompanied by authorized employees.

40. Physical access to the critical systems shall be revoked immediately if the same is no longer required.

41. The MIIs shall ensure that the perimeter of the critical equipment room is physically secured and monitored by employing physical, human, and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate. The MIIs shall establish guidelines for the retention of data captured by CCTV, card access systems, and similar sources.

Network Security Management

42. The MIIs shall establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices, and enterprise mobile devices within the IT environment. The MIIs shall conduct regular enforcement checks to ensure that the baseline standards are applied uniformly.

43. The MIIs shall install network security devices, such as firewalls as well as intrusion detection and prevention systems, to protect its IT infrastructure from security exposures originating from internal and external sources.

44. Anti-virus software shall be installed on servers and other computer systems. The MIIs shall ensure Endpoint Detection and Response (EDR)/ Endpoint Protection Platform (EPP), antivirus and anti-malware software and signatures are up to date on all IT systems.

45. The MIIs shall use application directory whitelisting on all assets to ensure that only authorized software is run, and all unauthorized software is blocked from installations/executing.

46. The MIIs shall build effective network segregation for containing cyber incidents and minimizing disruption to business operations. Internet web browsing provides a conduit for cyber criminals to access the IT systems. In this regard, the MIIs shall consider isolating internet web browsing activities from its endpoint devices using physical or logical controls, or implement equivalent controls, so as to reduce exposure of its IT systems to cyber-attacks.

47. The MIIs shall apply appropriate network segmentation / isolation techniques to restrict access to sensitive information, hosts, and services. Segment-to-segment access shall be based on a strong access control policy and the principle of least privilege.

48. The MIIs shall deploy web and email filters on the network. These devices shall be configured to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses, malicious domains/URLs at the firewall. All emails, attachments, and downloads both on the host and at the mail gateway shall be scanned with a reputable antivirus solution.

49. The network devices of the MIIs shall be configured in line with the whitelist approach of IPs, ports, and services for inbound and outbound communication with proper Access Control List (ACL) implementation.

50. The MIIs shall implement DNS filtering services to ensure clean DNS traffic is allowed in the environment. DNS security extension for secure communication shall be used.

51. Management of critical servers/ applications/ services/ network elements shall be restricted through enterprise-identified intranet systems.

52. MIIs shall implement comprehensive email security measures that prevent email spoofing, phishing, and Business Email Compromise (BEC) attacks through the deployment of industry-standard email authentication protocols.

53. The MIIs shall ensure that all log sources are being identified, and their respective logs are being collected. An indicative list of types of log data to be collected is as follows.

    i. System logs
    ii. Application logs
    iii. Network logs
    iv. Database logs
    v. Security logs
    vi. Performance logs
    vii. Audit trail logs
    viii. Event logs

    In order to identify unusual patterns and behaviours, monitoring of all logs of events and incidents shall be done.

54. Strong log retention policy, shall be implemented as per the extant applicable government guidelines/ policies/ laws/ circulars/ regulations, etc. issued by the Government of India (GoI) / IFSCA such as The IT Act 2000, Digital Personal Data Protection Act (DPDP) 2023, and as required by CERT-In, NCIIPC or any other government agency.

Awareness and Training

55. The MIIs shall get onboarded to National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cybersecurity threats.

56. The MIIs shall conduct periodic training programs to enhance awareness levels among the Board, employees, outsourced staff, vendors, etc. on IT / Cyber security policy and standards.

57. The training program shall be reviewed and updated at regular intervals to ensure that the contents of the program remain current and relevant. The review shall take into consideration changes in MII's cyber security policies, prevalent and emerging risks, and the evolving cyber threat landscape.

58. The MIIs shall also establish a comprehensive training and awareness program on mitigation relating to post-quantum risk.

Data Security

59. Data shall be encrypted in motion, at rest, and in-use by using encryption methods.

60. The MIIs shall deploy Data Loss Prevention (DLP) solutions/ processes.

61. The MIIs shall implement necessary measures to prevent unauthorized access, copying, or transmission of data / information held in a contractual or fiduciary capacity. It shall be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.

62. The information security policy shall also cover the use of devices that can be used for capturing and transmission of sensitive data within their IT infrastructure.

63. The MIIs shall permit only authorized data storage devices through appropriate validation processes.

64. Security measures shall be implemented to prevent and detect the use of unauthorized internet services that allow users to communicate or store confidential data. Examples of such services include social media, cloud storage and file sharing, emails, and messaging applications. The MIIs shall ensure appropriate controls are implemented in environments to manage the access and removal of such data to prevent data leakage. Wherever possible, such data shall be masked in the test and development environments.

65. The use of sensitive production data in non-production environments shall be restricted. In exceptional situations where such data needs to be used in non-production environments, proper approval has to be obtained from the CISO.

66. The MIIs shall maintain offline, encrypted backups of data and shall regularly test these backups at least on a quarterly basis to ensure confidentiality, integrity, and availability.

67. The MIIs shall ensure all cryptographic algorithms used have been subject to rigorous testing or vetting to meet the identified security objectives and requirements.

68. The MIIs shall establish cryptographic key management policy, standards, and procedures covering key generation, distribution, installation, renewal, revocation, recovery, and expiry.

69. The MIIs shall monitor developments in the area of cryptanalysis and, where necessary, update or change the cryptographic algorithms or increase the key lengths to ensure they remain resilient against evolving threats.

    For example, the Advanced Encryption Standard (AES), a predominant symmetric cipher, deems its 256-bit key sizes as quantum-resistant. In light of increasing "Harvest Now, Decrypt Later" attacks, utilizing AES in encryption can protect critical data even in the long term if and when Quantum Computing threatens current encryption standards. Similarly, awareness of developments in Post-Quantum Cryptography (PQC) can help an entity transition to the post-quantum world without endangering its critical systems.

70. The MIIs shall implement DLP measures on personal computing or mobile devices that are used to access MII's IT systems and networks. Two common ways to address this are the use of Mobile Device Management (MDM) or Mobile Application Management (MAM), as well as virtualization solutions. These solutions can be augmented with other security measures for personal devices to provide enhanced functionalities.

Hardening of Hardware and Software

71. The MIIs shall only deploy hardened and vetted hardware/ software. During the hardening process, the MIIs shall, inter-alia, ensure that default usernames and passwords are replaced with non-standard usernames and strong passwords and that all unnecessary services are removed or disabled in the software/ system.

72. For running services, non-default ports shall be used wherever applicable. Open ports on networks and systems, that are not in use or can be potentially used for the exploitation of data, shall be blocked. All open ports shall be monitored, and appropriate measures shall be taken to secure them.

73. The practice of whitelisting ports based (at the firewall level) on business usage shall be implemented rather than blacklisting certain ports. Traffic on all other ports which have not been whitelisted shall be blocked by default.

74. The MIIs shall perform Vulnerability Assessment and Penetration Testing (VAPT) before the commissioning of new systems and/or any production release, especially those that are part of critical systems or connected to critical systems.

75. Revalidation of VAPT post closure of observations shall be done in a time-bound manner to ensure that all the open vulnerabilities have been fixed.

Change Management Process

76. The MIIs shall have a clearly defined framework for change management including requirements justifying exception(s), duration of exception(s), process of granting exception(s), and authority for approving and for periodic review of exception(s) given.

77. The change management process shall also be part of all agreements with third-party service providers to ensure that changes to the system are implemented in a controlled and coordinated manner.

78. The Change Management process shall include (but not be limited to) submission, planning (impact analysis, rollout plan), approval, and implementation, review (post-implementation), closure, etc.

Application testing and Secure Software Development

79. The MIIs shall ensure that regression testing is undertaken before new or modified systems are implemented. The scope of tests shall cover business logic, security

controls, and system performance under various stress-load scenarios, and recovery conditions.

80. To ensure the secure rollout of software and applications, the MIIs shall conduct threat modelling and application security testing during development, incorporating relevant security requirements from established standards and guidelines such as OWASP Application Security Verification Standard (OWASP-ASVS).

81. The MIIs shall adopt and implement multiple layers of security controls to protect systems and data effectively.

82. MIIs shall have API security solutions in place for securing services and data transmitted through APIs. Proper access management, and effective authentication and authorization shall be done to ensure that only the desired entities have access to the APIs. While developing APIs, OWASP top 10 API security risks shall be mitigated and connecting to entities via APIs shall be strictly on a whitelist-based approach.

Vulnerability Assessment and Penetration Testing (VAPT)

83. The MIIs shall regularly conduct vulnerability assessments to detect security vulnerabilities in the IT environment. The MIIs shall also carry out periodic penetration tests, at least once in a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.

84. For the MIIs, whose systems have been identified as "protected systems" by NCIIPC, the VAPT exercise shall be conducted at least twice in a financial year.

85. Remedial actions shall be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.

Remote Access Management

86. The MIIs shall ensure a proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources securely from outside the physical premises of the MIIs using an internet connection.

87. The MIIs shall ensure that only trusted client machines shall be permitted to access enterprise IT resources remotely. The MIIs shall put in place appropriate security control measures such as (including but not limited to) host integrity

check, binding of the MAC address of the device with the IP address, etc. for remote access and telecommuting.

88. The MIIs shall ensure that appropriate risk mitigation mechanisms are put in place whenever remote access to IT resources is permitted for third-party service providers.

89. The MIIs shall ensure that remote access is monitored continuously for any abnormal/ unauthorized access, and appropriate alerts and alarms shall be generated to address this breach before any damage is done.

90. The MIIs shall implement robust VPN solutions, which provide strong encryption and two or more layers of protection, to protect the integrity of data transmitted between remote users' devices and internal systems. The MIIs are also encouraged to implement double/multiple VPN servers for additional protection ("VPN Server Chaining").

91. The MIIs shall implement strong authentication, such as multi-factor authentication, for users performing remote access to safeguard against unauthorized access to the IT environment of MIIs.

Patch Management

92. The MIIs shall establish a patch management policy to ensure that all applicable patches (at both PDC and DR Site) are identified, assessed, prioritized, tested, and applied to all IT systems/applications within the time limit as defined below. However, for emergency patching, patches shall be deployed within timelines as stipulated by the OEMs.

Sr. No.	Criticality of Patch	Timeline
1	High	1 Week
2	Moderate	2 Weeks
3	Low	1 Month

93. The patch management policy shall be approved by SCOT of the MIIs and shall be reviewed by SCOT for the MIIs at least on an annual basis.

94. All operating systems and applications shall be updated with the latest patches on a regular basis. As an interim measure for zero-day vulnerabilities, and where patches are not available, virtual patching may be considered for protecting systems and networks. Constraints due to which virtual patching is done shall be

legitimate and documented. Patches shall be sourced only from the authorized sites of the OEM.

95. All patches shall be tested first in a non-production environment which shall be identical to the production environment.

96. Hardware and software of critical systems shall be replaced before they reach End-of-Life/End-of-Support.

97. Compensatory controls like virtual patching shall be implemented for legacy systems for a maximum period of 6 months. Further, the constraints due to which virtual patching is done shall be legitimate and documented.

Disposal of systems and storage devices

98. The MIIs shall frame suitable policies for disposals of the storage media and systems. The data / information on such devices and systems shall be erased by using methods viz. wiping / shredding/ cleaning / overwrite, degauss and physical destruction, as applicable.

Management of Third-party Risks

99. The MIIs shall implement a risk-based approach with respect to outsourcing and third-party risk management.

100. The MIIs shall have an effective process for managing third-party cyber security risks through the entire third-party risk management life cycle.

101. The MIIs shall take appropriate steps to ensure that third parties have in place a comprehensive cyber security and cyber resilience program and have similar standards of Information Security as is applicable to the MII itself.

102. Before entering new third-party relationships and during the lifespan of the engagement, the MIIs shall conduct cyber security risk assessments and due diligence to consider whether these relationships are consistent with their cyber security and cyber resilience strategy.

103. The MIIs' contracts with their third parties shall include terms and conditions to support the management of cyber security risks and include cyber security risks stemming from subcontracting.

104. In situations where the MIIs are dependent on a single service provider for material or critical outsourced tasks, the risks arising therein shall be identified

and managed effectively. The MIIs need to take into account concentration risk while outsourcing multiple critical services to the same third-party service provider. Accordingly, the MIIs shall prescribe specific cybersecurity controls, including audits of their systems and protocols from independent auditors, to mitigate such concentration risk.

105. In situations where the MIIs are aware that one service provider provides material or critical outsourcing services to multiple regulated entities including MIIs themselves, the risks arising therein shall be identified and managed effectively.

106. The MIIs shall maintain an inventory of their third parties and identify Critical Service Providers. A Critical Service Providers is a service provider that has a direct contractual arrangement with an entity, to provide, on a continuous basis, services to that entity (and potentially its participants), which are essential for ensuring information confidentiality and integrity and service availability, as well as the smooth functioning of its core operations.

107. The MIIs shall monitor changes in criticality and risk, and review contract performance of third parties on an ongoing basis to manage their cyber security risks.

108. The MIIs shall have appropriate contingency plans and exit strategies in place to address situations where third parties fail to meet cyber-related performance expectations or pose cyber security risks outside the MII's risk appetite.

Cloud Security Control

109. The MIIs are required to create a comprehensive cloud security policy. While framing cloud security controls, the MIIs are encouraged to use a layered approach toward cloud security, covering all the layers, which are:

i. Data
ii. Application
iii. Host/Compute
iv. Network
v. Identity and Access
vi. Physical and Perimeter

110. In the event the MIIs are utilizing the services from multiple cloud service providers, it is required to have relevant personnel who possess the necessary understanding of the corresponding cloud solutions. Further, the MIIs are required to address the following challenges:

i. Ensuring data protection and privacy for each environment
ii. Understanding how different solutions fit together
iii. Understanding service integration options
iv. Loss of visibility and control

111. As cloud computing follows the shared responsibility model, Cloud Service Providers (CSPs) are responsible for maintaining the security and sanctity of the physical data center along with IT infrastructure (compute, network, storage, security) deployed for the cloud while the entities are responsible for framing and institutionalizing proper security controls, while understanding the underlying risks.

IV. Detect

112. To ensure high resilience, high availability, and timely detection of attacks on systems and networks, the MIIs shall implement suitable mechanisms to monitor the capacity utilization of critical systems and networks.

113. The MIIs shall establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events/ alerts and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access, and unauthorized copying and transmission of data/ information held in a contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications, and network devices exposed to the internet shall also be monitored for anomalies.

114. Suitable alerts shall be generated in the event of the detection of unauthorized or abnormal system activities, transmission errors, or unusual online transactions.

V. Respond

115. The MIIs are advised to formulate a Cyber Crisis Management Plan (CCMP) based on the architecture deployed, threats faced and the nature of operations. The CCMP shall define the various cyber events, incidents, and crises faced by the MIIs, the extant cyber threat landscape, the cyber resilience envisaged, incident prevention, cyber crisis recognition, mitigation, and management plan. The CCMP shall be approved by the SCOT of the MIIs and the Board of the MIIs. The CCMP shall also be reviewed and updated annually.

116. The MIIs shall develop an Incident Response Management Plan as part of their CCMP. The response plan shall define responsibilities and actions to be

performed by its employees and support/ outsourced staff in the event of a cyber-attack or cybersecurity incident.

117. Any cyber-attack, cybersecurity incident, and/ or breach shall be notified to IFSCA and CERT-In within 6 hours of noticing/ detecting such incidents or being brought to notice about such incidents. This information shall be shared with IFSCA through the cyber-incidents@ifsca.gov.in within 6 hours.

118. The MIIs shall submit the interim report within 3 days followed by a detailed root cause analysis report within 30 days. The MIIs shall take mitigation measures for the same within 7 days.

119. The incident shall also be reported to CERT-In in accordance with the guidelines/ directions issued by CERT-In from time to time. Additionally, the MIIs, whose systems have been identified as "Protected systems" by NCIIPC shall also report the incident to NCIIPC.

120. The quarterly reports containing information on cyber-attacks, threats, cybersecurity incidents, and breaches experienced by the MIIs and measures taken to mitigate vulnerabilities, threats, and attacks including information on bugs/ vulnerabilities, and threats, shall be submitted to IFSCA within 15 days from the quarter ended June, September, December, and March of every year.

121. For the purpose of coordinating incident response, the MIIs shall regularly update the contact details of service providers, intermediaries, and other stakeholders.

122. The MIIs shall collect and preserve data related to the incident, such as system logs, network traffic, forensic images, etc., of affected systems in and secure and forensically sound manner.

VI. Recover

123. A recovery plan shall be formulated by the MIIs and approved by their respective SCOT for the MIIs. The backup and recovery plan shall include policies and software solutions that work together to maintain business continuity in the event of a security incident. Such a plan shall include guidance on the restoration of data with the backup software used by the MIIs.

124. The recovery plan of the MIIs shall have plans for the timely restoration of systems affected by incidents of cybersecurity incidents/ attacks or breaches. The recovery plan shall be in line with the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) specified by IFSCA's Guidelines for Business

Continuity Plan (BCP) and Disaster Recovery (DR) for Market Infrastructure Institutions (MIIs), amended from time to time.

VII. Resilience

125. The MIIs shall perform cyber resilience testing by undertaking regular business continuity drills and specific scenario exercises at least once in a financial year to check the readiness of the organization and the effectiveness of existing security controls at the ground level. This shall assess the effectiveness of people, processes and technologies to deal with such attacks. The said scenarios may be devised by the MIIs in consultation with their respective SCOTs. Critical third-party service providers may also be included in the cyber resilience testing.

126. The result of the cyber resilience testing shall be placed before SCOT for the MIIs. The lessons learned from conducting such cyber resilience testing shall be shared with IFSCA within 3 months from the end of the financial year.

VIII. Cyber Security Operation Center (C-SOC)

127. MIIs shall have a Cyber Security Operation Center (C-SOC) that would be a *24x7x365* set-up manned by dedicated security analysts.

128. In order to build an effective C-SOC, MIIs shall have appropriate mix of right people, suitable security products, and well-defined processes and procedures.

129. The MII shall ensure that the governance and reporting structure of the C-SOC is commensurate with the risk and threat landscape of the MII.

130. The MIIs shall also build a contingent C-SOC at their respective DR sites with identical capabilities with respect to. the primary C-SOC.

IX. Periodic Audit

131. The MIIs shall engage only CERT-In empanelled Information Security (IS) auditor for conducting external audits including cyber audits to audit the implementation of all provisions mentioned in these guidelines.

132. A CERT-In empanelled IS auditing organization can audit the MIIs for a maximum period of three consecutive years. Subsequently, the said IS auditing organisation shall be eligible for auditing the MIIs again only after a cooling off period of two years.

133. The auditor engaged by the MIIs shall not have any conflict of interest with the MIIs. The audit shall be conducted annually and a report in this regard shall be submitted to IFSCA by the MIIs within 90 days from the end of the financial year.

134. Though the minimum audit frequency prescribed is annual, the MIIs may choose to adopt a higher frequency commensurate with their cyber risks and the criticality of their systems.

135. Along with the cyber audit reports, the MIIs shall also submit a declaration from the Managing Director (MD)/ Chief Executive Officer (CEO) in this regard.

136. All MIIs shall obtain ISO 27001 certification within 2 years of the issuance of these guidelines. The evidence of certification shall be submitted along with the cyber security audit report to IFSCA.

137. To ensure that all the open vulnerabilities in the IT assets of the MIIs have been fixed, revalidation VAPT and cyber audit shall also be done in a time-bound manner.

138. The Audit Management process of the MIIs shall include (but not be limited to) audit program/ calendar, planning, preparation, delivery, evaluation, reporting, and follow-up, etc.

139. IFSCA shall at any time perform search and seizure of the IT resources of the MIIs storing/ processing data and other relevant IT resources (including but not limited to logs, user details, etc.) pertaining to the MIIs. In this process, IFSCA or IFSCA-authorized personnel/ agency may access MII's IT infrastructure, applications, data, and documents, including other necessary information given to, stored, or processed by third-party service providers.

***