CIRCULAR

IFSCA-CSD/MSC/2/2026-DCS **April 20, 2026**

To,

All the Stock Exchanges, including Bullion Exchange, in the International Financial Services Centres (IFSC)

All the Clearing Corporations in the International Financial Services Centres (IFSC)

All the Depositories in the International Financial Services Centres (IFSC)

Dear Madam/Sir,

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

1. IFSCA vide circular dated March 10, 2025 had issued the 'Guidelines on Cyber Security and Cyber Resilience for Regulated Entities in IFSCs', prescribing a minimum baseline framework for cyber security applicable to all Regulated Entities (REs) operating within GIFT IFSC. The said framework adopts a principles-based approach to ensure proportional applicability, taking into account the heterogeneity of REs in terms of size, structure, complexity and risk profile.

2. The Market Infrastructure Institutions (MIIs) comprising Stock Exchanges, Clearing Corporations, Depository and the Bullion Exchange are systemically critical to the stability, integrity and continuity of the capital market in IFSC. In view of their central role and heightened risk exposure, a more robust, granular and prescriptive cyber security framework is warranted.

3. Accordingly, with a view to enhancing cyber resilience, mitigating systemic cyber risks and ensuring preparedness against evolving threat vectors, IFSCA has formulated the "Guidelines on Cyber Security and Cyber Resilience for Market Infrastructure Institutions (MIIs) in IFSC" as set out in Annexure A.

4. The key objective of these Guidelines is to establish a comprehensive cyber security and cyber resilience framework for the MIIs operating in IFSC. The Guidelines seek to:

a. strengthen governance and reinforce accountability for cyber security at the Board and Senior Management level
b. address evolving cyber threat landscape, including emerging risks such as those arising from developments in quantum computing
c. align MII cyber security practices with national and international standards and
d. ensure robust incident detection, response, reporting and recovery mechanisms.

5. These Guidelines are structured around the following cyber security functions:

    a. Govern
    b. Identify
    c. Protect
    d. Detect
    e. Respond
    f. Recover
    g. Resilience.

6. These Guidelines shall come into effect from April 01, 2026. The MIIs shall ensure full compliance within the timelines specified in the respective provisions of these Guidelines.

7. This Circular is issued in exercise of powers conferred by Sections 12 and 13 of the International Financial Services Centres Authority Act, 2019, to develop and regulate the financial services market in the International Financial Services Centre.

A copy of this circular is available on the website at www.ifsca.gov.in

Yours Faithfully,

Praveen Kamat
General Manager & Chief Information Security Officer
Division of Cyber Security
Email: praveen.kamat@ifsca.gov.in
Tel : +91- 079 - 61809820

Annexure A

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

Financial institutions today face a constant barrage of threats that attempt to compromise the Confidentiality, Integrity and Availability (CIA) of their computer systems, networks and databases. To counter this, it is imperative that a financial institution have a robust Cyber security framework in place that includes measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience i.e. the capacity to maintain operations during a cyberattack and recover swiftly after a breach.

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. The said policy shall also cover the mechanism for handling exceptions to the proposed framework. Furthermore, the Board shall periodically review the Policy document to ensure that the framework remains adaptive to emerging threats, in order to strengthen and improve the MII's cyber security and cyber resilience posture.

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 cyber security 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 Standing Committee on Technology (SCOT) of the MIIs shall review the implementation of the Policy on a bi-annual basis.

6. For MIIs that have been identified as Critical Information Infrastructure (CII) by the 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.

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

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

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

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

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

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

11. The MIIs shall formally define and document the cyber security obligations for all individuals, who possess authorized access to the systems or networks of the MII, inter alia, including its:

    a. internal employees,
    b. outsourced personnel,
    c. third-party vendors,
    d. market participants.

II. Identify

12. The MIIs shall identify and maintain an up-to-date inventory of information assets, including data, applications and third-party dependencies. This may also include a list of:

    a. digital assets (such as URLs, domain names, applications, APIs, etc.),
    b. shared resources (including cloud assets),
    c. interfacing systems (internal and external),
    d. details of its network resources,
    e. connections to its network and data flows.

13. Any additions/ deletions or changes in existing assets shall be reflected in the asset inventory in a timely manner.

14. 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, inter alia, include:

    a. business-critical systems,
    b. internet-facing applications /systems,
    c. systems that contain sensitive data,
    d. sensitive personal data,
    e. sensitive financial data,
    f. Personally Identifiable Information (PII)

    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 at least once a year.

15. The MII shall identify, categorize and quantify cyber security threats and vulnerabilities that it may face, along with the probability of occurrence and the potential systemic impact on business continuity. The MII shall put in place technical and administrative controls that are strictly commensurate with the criticality of the identified risks and the sensitivity of the underlying assets.

16. The MIIs shall prepare and maintain an up-to-date network architecture diagram at the organizational level that include both wired and wireless networks.

17. The MIIs shall conduct a risk assessment (including post-quantum risks) of the IT environment of their organization on an annual basis to acquire visibility and a reasonably accurate assessment of the overall cyber security risk posture.

III. Protect

Access Controls

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

19. 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 (PoLP). Such access shall be authorized using strong authentication mechanisms and shall be immediately revoked upon expiration of the required period.

20. The MIIs shall implement strong password controls for users' access to systems, applications, networks and databases. Password controls shall include:

    a. a change of password upon first log-on,
    b. minimum password length and history,
    c. password complexity and
    d. maximum validity period.

    The stored user credential data shall be protected using industry-standard, collision-resistant cryptographic hashing algorithms.

21. The User access rights, delegated access, unused tokens, and privileged user activities shall be reviewed on a quarterly basis for critical systems and bi-annually for non-critical systems.

22. 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.

23. The MIIs shall ensure that all critical systems accessible over the internet are shielded by a Defense-in-Depth (DiD) architecture.

24. 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.

25. To mitigate the risk of internal compromise and unauthorized system changes, 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 or alter security configurations.

26. 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.

27. 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

28. The MIIs shall implement a rigorous oversight framework for all personnel (including permanent staff, outsourced staff, and third-party service providers) possessing authorized access to critical IT assets. Such access shall be governed by PoLP and shall be subject to real time session monitoring and automated alerting.

Security of Domain Controllers (DCs)

29. Given that threat actors often target and use Domain Controllers (DCs) for staging network-wide attacks, the MIIs shall implement the following structural safeguards.

    a. The MII shall ensure application of all released security patches to DCs in a timely manner.
    b. The MII shall ensure that no non-essential software is installed on DCs.
    c. The MII shall ensure that access to DC is restricted and controlled.

30. The MII shall undertake rigorous internal and external Red Team simulations specifically targeting known Active Directory Domain Controller abuse attacks. Any identified vulnerabilities or misconfigurations shall be classified by risk severity and shall be remediated on a priority basis.

Insider Threat

31. An Insider threat shall, inter alia, include acts such as:

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

32. As the human element plays an important role in managing IT systems and processes in an IT environment, the MII shall ensure that all personnel, including contractors and service providers, have the requisite level of cyber and information security awareness and training to perform their tasks while considering cyber security risks.

Physical security

33. Physical access to the critical systems shall be restricted and access shall be supervised by ensuring that visitors remain under the direct supervision of an authorized official at all times.

34. The MIIs shall implement a Role-Based Access Control (RBAC) framework for all physical access to critical systems.

35. The MIIs shall ensure that the perimeter of the critical equipment room is physically secured and monitored by employing physical, human, and procedural controls (for example, security guards, CCTVs, card access systems, mantraps, bollards, etc.) where appropriate. The MIIs shall establish a Data Retention Policy for all surveillance and access logs (CCTV, card swipes), to ensure that such records are preserved for a period sufficient to support forensic investigations and regulatory audits.

Network Security Management

36. 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.

37. 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.

38. The MIIs shall ensure that all IT systems are protected by antivirus, anti-malware and Endpoint Detection and Response (EDR) / Endpoint Protection Platforms (EPP) solutions. In the case of Linux or other non-Windows Operating Systems where such solutions pose documented compatibility or performance constraints, the MIIs shall implement compensatory controls to ensure that there is no degradation in the institutional security posture. The MIIs shall ensure that the EDR/EPP, antivirus and anti-malware solutions and signatures are up to date on all IT systems.

39. The MIIs shall implement an enterprise-wide Application Whitelisting (AWL) mandate. Appropriate mechanisms shall be implemented to proactively block the installation or execution of unauthorized software.

40. 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.

41. 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 PoLP.

42. The MIIs shall implement Secure Web Gateways (SWG) and Email Security Appliances (ESA) to regulate all inbound and outbound traffic.

43. 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.

44. 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.

45. The management of critical servers/ applications/ services/ network elements shall be restricted through enterprise-identified intranet systems.

46. The MIIs shall implement an enterprise-wide email security measures to eliminate the risk of spoofing, phishing, and Business Email Compromise (BEC).

47. The MIIs shall maintain a definitive inventory of all log generating assets. An indicative list of types of logs 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

    The MIIs shall put in place necessary systems for automated monitoring of all aggregated logs and security telemetry. This monitoring system must be capable of performing User and Entity Behaviour Analytics (UEBA) to identify deviations from established baselines and detect sophisticated, unusual patterns and behaviours, that evade traditional threshold-based alerts.

48. To fulfil institutional accountability, MIIs shall establish strong log retention policy that is in alignment with the extant applicable guidelines/ policies/ laws/ circulars/ regulations, etc. issued by the Government of India (GoI) / IFSCA such as:

a. The Information Technology Act 2000,
b. The Digital Personal Data Protection Act (DPDP) 2023,
c. Guidelines issued by CERT-In, NCIIPC or any other government agency,
d. Guidelines issued by IFSCA

Awareness and Training

49. The MIIs shall complete their onboarding with the National Cyber Coordination Centre (NCCC).

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

51. 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.

52. The MIIs shall implement a specialized training and awareness program focused on Post Quantum Cryptography (PQC). This program shall ensure that the technical personnel and risk officers are proficient in identifying quantum-vulnerable algorithms and are prepared to execute the transition to PQC standards as defined by international and national bodies (e.g., MeitY, CERT-In, NQM, NIST).

Data Security

53. The data in motion and data at rest shall be encrypted using strong cryptographic algorithms.

54. To safeguard against internal and external data breaches, the MIIs shall enforce Data Loss Prevention (DLP) controls across data in use, data in motion and data at rest.

55. 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.

56. 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.

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

58. 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, appropriate approval shall be obtained.

59. The MIIs shall maintain offline, encrypted backups of data and shall test these backups periodically to ensure confidentiality, integrity, and availability.

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

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

62. The MIIs shall conduct an annual Cryptographic Risk Assessment to evaluate the continued efficacy of their encryption algorithms against advancements in cryptanalysis and Quantum Computing / High Performance Computing.

    The MIIs shall establish a roadmap for the adoption of PQC standards (e.g. NIST FIPS 203, 204 and 205) to ensure seamless migration of critical systems before existing asymmetric standards are rendered obsolete by advancements in Quantum Computing / High Performance Computing.

63. 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

64. The MIIs shall deploy hardware and software assets that have undergone a formal security vetting and hardening process. The MIIs shall maintain a log of hardening

activities, verifying that no IT system retains default administrative credentials or active, unmonitored backdoors.

65. 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.

66. 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.

67. 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.

68. 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

69. 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.

70. 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.

71. 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.

Application testing and Secure Software Development

72. 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.

73. 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).

74. To safeguard institutional data, the MIIs shall implement necessary technical controls to ensure that all Application Programming Interfaces (APIs) adhere to secure by design principles. The MIIs shall ensure that all API connectivity is restricted to authorized entities. Furthermore, all API development shall factor in the mitigation of the Open Worldwide Application Security Project (OWASP) API Security Top 10 vulnerabilities, prior to deployment in production environment.

Vulnerability Assessment and Penetration Testing (VAPT)

75. 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, to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.

76. As part of the VAPT, the MIIs shall 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.

77. For those MIIs, whose systems have been identified as "protected systems" by NCIIPC, the VAPT exercise shall be conducted on a bi-annual basis. All testing must align with the guidelines prescribed by NCIIPC and CERT-In.

78. The MIIs shall take remedial actions to address the gaps identified during the VAPT, within defined timelines. The remediation process shall be prioritized on the basis of business criticality and threat severity.

Remote Access Management

79. 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.

80. 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 for remote access and telecommuting.

81. 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.

82. 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.

Patch Management

83. 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 defined timelines. However, for emergency patching, patches shall be deployed within timelines as stipulated by the OEMs.

84. 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.

85. 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. Patches shall be sourced only from the authorized sites of the OEM.

86. The MIIs may choose to adopt appropriate periodicity commensurate with their cyber risks and the criticality of their systems for implementing Compensatory controls for legacy systems.

Disposal of systems and storage devices

87. 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

88. The MIIs shall implement a risk-based approach to manage its cyber security risk with respect to outsourcing and third-party risk management.

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

90. The MIIs shall take appropriate steps to ensure that third parties have in place a comprehensive cyber security and cyber resilience program.

91. Prior to entering into 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.

92. The MIIs' contracts with third party entities shall include the necessary terms and conditions to support the management of cyber security risks. These contracts shall prohibit the subcontracting of critical functions without the explicit written consent of the MIIs.

93. 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 are required to take into account concentration risk while outsourcing multiple critical services to the same third-party service provider. Accordingly, the MIIs shall prescribe specific cyber security controls, including audits of their systems and protocols from independent auditors, to mitigate such concentration risk.

94. The MIIs shall maintain a comprehensive inventory of all third-party service providers. The MIIs shall categorize and designate Critical Service Providers (CSPs) based on their operational impact. A CSP 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.

95. 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

96. 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

97. 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

98. As cloud computing follows the shared responsibility model, cloud service providers 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

99. 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.

100. 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.

101. 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

102. 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.

103. 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 cyber security incident.

104. Any cyber-attack, cyber security 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 cyber-incidents@ifsca.gov.in.

105. 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 from detection of the incident.

106. 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.

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

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

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

VI. Recover

110. 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.

111. The recovery plan of the MIIs shall have plans for the timely restoration of systems affected by cyber security 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

112. 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.

113. The MIIs shall place the results of the cyber resilience testing before their SCOT. 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)

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

115. The MIIs may choose any of the following models:

i. A standalone C-SOC,
ii. C-SOC shared by the MII with its group/ parent entities (that are also recognised MIIs),
iii. C-SOC that may be shared by the MII with other recognised MII(s).

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

IX. Periodic Audit

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

118. 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.

119. 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 120 days from the end of the financial year.

120. 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.

121. 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.

122. All MIIs shall obtain ISO 27001 certification within 2 years of the issuance of these guidelines. The evidence of certification shall be submitted to IFSCA.

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

124. 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.

125. 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.

***