NOTICE

Subject: **GUIDANCE FOR REGULATED ENTITIES ON ESTABLISHING AND MAINTAINING A CYBER RESILIENCE FRAMEWORK**

The public is advised that the Commission *En Banc,* in its meeting held on 16 December 2025, resolved to expose the draft Memorandum Circular on *GUIDANCE FOR REGULATED ENTITIES ON ESTABLISHING AND MAINTAINING A CYBER RESILIENCE FRAMEWORK.*

The Commission hereby requests for comments, suggestions and/or inputs from all concerned on the proposed draft Memorandum Circular by submitting written comments on or before **16 January 2026** through email at ipsd msrd@sec.gov.ph, eavalencia@sec.gov.ph and ggjarugay@sec.gov.ph with our proposed subject of **"COMMENTS ON THE PROPOSED GUIDANCE FOR REGULATED ENTITIES ON ESTABLISHING AND MAINTAINING A CYBER RESILIENCE FRAMEWORK."**

Issued on 17 December 2025.

SEC MEMORANDUM CIRCULAR NO. _____
Series of 2025

TO	:	**ALL CONCERNED**
SUBJECT	:	**GUIDANCE FOR REGULATED ENTITIES ON ESTABLISHING AND MAINTAINING A CYBER RESILIENCE FRAMEWORK**
DATE	:	**___ December 2025**

WHEREAS, Section 5 (b) of the Securities Regulation Code (SRC) provides that the Commission has the power to formulate policies and recommendations on issues concerning the capital markets;

WHEREAS, Section 8 (g) of the Financial Products and Services Consumer Protection Act (FCPA) mandates financial regulators to prescribe the minimum information security standards for compliance by all financial service providers. Financial service providers are also mandated to adopt and implement information security standards to ensure the safety and protection of the confidentiality, integrity, availability, authenticity, and non-repudiation of the client's information and financial transactions and to ensure the data privacy of their clients.

WHEREAS, the National Cybersecurity Plan 2023-2028 ("NCSP") states that the Philippine government regards cybersecurity as critical, not only to peace and security but also to economic development.

WHEREAS, the Securities and Exchange Commission (the "Commission") acknowledges the pronouncement in the Philippine Development Plan 2023-2028 ("PDP") that the rapid growth and sophistication of cybercrimes and cyber-attacks have increased the vulnerability of data, people, and structures.

WHEREAS, in line with the NCSP, the Commission recognizes the importance of cybersecurity in ensuring public trust in e-Commerce and online banking and trade. As such, the Commission acknowledges that institutionalizing trust by strengthening the capability to secure transactions in cyberspace is undeniably important to the country's economic growth.

WHEREAS, the Commission likewise acknowledges the importance of establishing comprehensive cybersecurity regulations to protect investors, promote market stability, and foster trust in the Philippine capital market.

WHEREFORE, IN VIEW OF THE FOREGOING, the Commission hereby promulgates the following guidelines:

SEC. 1. Coverage - These guidelines shall apply to Publicly Listed Companies, Broker Dealers, Investment Houses, Exchanges, Self-Regulatory Organization, Clearing Agencies, Securities Depositories, and Transfer Agents and other similar capital market participants.

SEC. 2. Definition of Terms – When used in this circular, the following terms are defined as follows:

2.1. **Availability -** Property of being accessible and usable upon demand by an authorized entity.

2.2. **Confidentiality –** Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

2.3. **Critical Information Infrastructure (CII) –** Computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data, and/or traffic data, that the incapacity or destruction of, or interference with such systems and assets would have a debilitating impact on economic security and/or the integrity of the capital markets.

2.4. **Cyber-attack –** Refers to an attack or attempt via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

2.5. **Cyber event –** Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.

2.6. **Cyber resilience framework –** Consists of the policies, procedures and controls to identify, protect, detect, respond to and recover from the plausible sources of cyber risks it faces.

2.7. **Cyber resilience strategy –** High level principles and medium-term plans to manage cyber risks.

2.8. **Cyber risk –** The combination of the probability of cyber incidents occurring and their impact.

2.9. **Cyber risk tolerance** - The propensity to incur cyber risk, being the level of cyber risk that a Covered Entity intends to assume in pursuing its strategic objectives.

2.10. **Cybersecurity –** The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets.

2.11. **Cybersecurity incidents/cyber incident –** A single or series of unwanted or unexpected information security (cybersecurity) events that have a significant probability of compromising business operations and threatening information security (cybersecurity).

2.12. **Cyberspace –** A complex environment emerging from the interaction of people, software, and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form

2.13. **Enterprise Risk Management -** An effective agency-wide approach to addressing the full spectrum of the organization's significant risks by

understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos.

2.14. Information system – Set of applications, services, information technology assets or other information-handling components, which includes the operating environment and networks.

2.15. Integrity - Property of accuracy and completeness.

2.16. Phishing - A form of social engineering where malicious actors attempt to fraudulently acquire sensitive information (such as login credentials, financial data, or personal information) by disguising as a trustworthy entity in an electronic communication (including but not limited to email, text message, or voice call).

2.17. Recovery Point Objective (RPO) – Refers to the maximum amount of data loss the organization can tolerate before business operations are significantly impacted.

2.18. Recovery Time Objective (RTO) – Represents the maximum acceptable downtime before full recovery must be completed.

2.19. Third-party service providers – Any unaffiliated person, company, or entity that performs services for the Covered Entity for a fee.

2.20. Threat – Potential cause of an unwanted incident, which may result in harm to a system, individual, or organization.

2.21. Vulnerability – Weakness of an asset or control that can be exploited by one or more threats.

SEC. 3. Establishing a Cyber Resilience Framework - Each Covered Entity shall adopt a cyber resilience framework that articulates its cyber resilience objectives and cyber risk tolerance, as well as procedures on how such Covered Entity effectively identifies, mitigates, and manages its cyber risks to support its objectives. Each cyber resilience framework shall be considered as continuously developing and Covered Entity shall make further efforts to adapt, evolve and improve their cyber resilience capabilities.

SEC. 4. Components of the cyber resilience framework - At the minimum, a cyber resilience framework of a Covered Entity shall be consistent with its enterprise risk management framework and shall integrate the following:

4.1. A cyber resilience strategy that meets the following standards:

4.1.1. Establishment of an internal, cross-disciplinary steering committee composed of senior management and appropriate staff from multiple business units to collectively develop a cyber resilience strategy and framework.

4.1.2. Shall be aligned with the Covered Entity's corporate strategy and other relevant strategies.

4.1.3. Approved by the Board of Directors of the Covered Entity (as may be endorsed and/or pre-approved by a committee specifically organized to manage matters involving the cyber

resilience framework) and regularly reviewed and updated according to the Covered Entity's threat landscape.

4.2. Roles, responsibilities and lines of accountabilities of the board of directors, the board committee, responsible person/s and key personnel involved in functions relating to the management of cyber risk (such as information technology and security, business units and operations, risk management, business continuity management and internal audit);

4.3. The identification, containment, analysis, eradication, recovery, and learning processes and procedures related to cyber breaches for purposes of decision- making;

4.4. Processes and procedures for the management of outsourcing, system development and maintenance arrangements with third-party service providers, including requirements for such third-party service providers to comply with the entity's information security policy; and

4.5. Communication procedures that will be activated by the entity in the event of a cyber breach, which include reporting procedures, information to be reported, communication channels, list of internal and external stakeholders and communication timeline.

SEC. 5. Cyber Risk Measures –Covered Entity shall ensure that comprehensive strategies and measures are in place to manage cyber risk. The following Cybersecurity Incident Response Model shall be adopted by Covered Entities in their respective cyber resilience frameworks:

5.1. **Identification.** A Covered Entity is expected to maintain an up-to-date inventory of all the critical functions, key roles, processes, information assets, third-party service providers and interconnections. It shall also have an enterprise risk management framework to identify risks and conduct risk assessments on a regular basis to determine, classify and document their level of criticality. Upon detection of a cyber incident, the Covered Entity's CERT shall immediately triage the incident, describe the event by answering the 5Ws and 1H (what, when, who, where, why, and how), noting that the question of "why" the incident happened may not yet be known. The CERT shall also assign a criticality level, and assign the issue resolution to a dedicated incident response agent or team.

5.2. **Containment.** A Covered Entity shall implement immediate, decisive, and time-sensitive measures to limit the magnitude and mitigate the potential spread of the cyber incident to other critical functions or information assets. The actions during this stage must be appropriate to the type of incident but shall include, at a minimum:

5.2.1. **Network Isolation.** Logical or physical segmentation of affected systems, networks or critical infrastructure to prevent unauthorized lateral movement.

5.2.2. **Access Revocation.** Immediate suspension or revocation of compromised credentials, accounts, and access keys.

5.2.3. **Quarantine.** Isolation of infected files, processes, or devices to prevent further execution or encryption.

The effectiveness of security controls shall be regularly assessed in order to adapt them to its evolving threat landscape. The controls must likewise be monitored and audited regularly to ensure that they remain effective and have been applied to all assets where they might be needed.

5.3. **Analysis.** A Covered Entity shall develop the appropriate investigative capabilities, including the people, processes and technology, to monitor and detect anomalous activities and events, and to determine the root cause and full scope of contained cyber incidents. This includes, but is not limited to, conducting forensic analysis of compromised assets, logs, and user activity to answer the questions of "why" the incident occurred and inform future prevention. A Covered Entity's monitoring and detection capabilities shall support information collection for the forensic investigation by ensuring that the security logs and relevant data are collected, protected, and backed up at a secure location with controls in place to mitigate the risk of alteration or destruction.

5.4. **Eradication.** A Covered Entity shall, based on the findings from the Analysis phase, remove the root cause of the incident from its environment and eliminate the threat actor's access. This includes, but is not limited to:

5.4.1. **Vulnerability Remediation.** Applying necessary patches, configuration changes, or procedural updates to close the exploit path.

5.4.2. **Threat Removal.** Complete removal of malicious code, unauthorized user accounts, or persistent access mechanisms (e.g., backdoors).

5.4.3. **Credential Reset.** Mandatory password/credential reset for all potentially compromised accounts.

This process is critical to ensure that the threat cannot immediately reinfect the system once containment is released and before recovery begins.

5.5. **Recovery.** A Covered Entity shall develop backup and recovery methods and strategies to be able to restore system operations with minimum downtime and limited disruption. In order to achieve its business continuity goals, a Covered Entity shall first define its RPOs and its RTOs, commensurate with its business requirements. Data necessary to replay participants' transactions shall be regularly backed up. Backups shall be protected at rest and in transit to ensure the confidentiality, integrity and availability of data, and shall be tested regularly to verify their availability and integrity. Crucially, before affected systems or services are fully restored for business use, the Covered Entity must perform validation checks to confirm that the threat has been completely removed and that the systems are operating securely, reliably, and in accordance with pre-incident security baseline configurations.

5.6. **Learning.** A Covered Entity shall have capabilities in place to gather information on common vulnerabilities, cyber threats, events and incidents occurring both within and outside the organization. As such, the Covered Entity shall be able to analyze the information gathered and assess the potential impact on its cyber resilience framework. The

Covered Entity shall distill and classify the lessons learned (e.g. strategic, tactical and operational), identify the key stakeholders to whom these apply, incorporate them to improve its cyber resilience framework and capabilities, and convey them to each relevant stakeholder on an ongoing basis.

SEC. 6. Governance. Covered Entity shall be able to comply with the following governance structure:

6.1. Its board of directors shall exercise oversight of risks from cybersecurity threats. If applicable, a Covered Entity shall have a board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and shall be able to describe the processes by which the board or such committee is informed about such risks.

6.2. The Covered Entity shall be able to identify its management's role in assessing and managing the registrant's material risks from cybersecurity threats. In doing so, the Covered Entity-should address, as applicable, the following non-exclusive items:

6.2.1. Which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;

6.2.2. The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and

6.2.3. Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

A Covered Entity's Board shall be primarily responsible for approving its cyber resilience framework and ensuring that cyber risk is effectively managed. The Board shall also be responsible in overseeing the creation or appointing a Computer Emergency Response Team (CERT), which can be in-house or outsourced.

SEC. 7. Establishment of a Computer Emergency Response Team – All Covered Entity shall establish its own CERT which shall be responsible in responding to cybersecurity incidents, regardless of their complexity or criticality. The CERT shall be responsible for the following:

7.1. Identification. Triage and classify cybersecurity incidents within the organization.

7.2. Containment and Analysis. Respond to cybersecurity incidents within the organization.

7.3. Eradication. For severe or critical cybersecurity incidents, coordinate the response with the NCERT.

7.**4. Recovery and Learning.** Develop and manage the cybersecurity response life cycle within the organization.

7.**5. Exercise.** Conduct cybersecurity tabletop simulations, drills, and exercises within the organization.

7.**6.** **Promotion of a cybersecurity culture.** Promote and train the organization in adopting a cyber-safe culture.

7.**7.** **Focal.** Act as the primary focal person of the organization to the nationwide network of CERT. The focal person to be appointed shall at least be a mid-level manager and shall serve as the primary contact for communications to and from the NCERT.

A Covered Entity's CERT shall have at least three (3) personnel, with a Chief Information Security Officer (CISO) position or equivalent that perform decision-making or management functions and information security officers, with sufficient cybersecurity trainings and credentials. Further composition of a Covered Entity's CERT may vary depending on the need and available resources of the organization. However, the team must be regularly upskilled in defensive security and incident management.

SEC. 8. Creation of a Chief Information Security Officer (CISO) – Each Covered Entity shall have a CISO position within the organization to lead the CERT. The CISO shall be the official responsible for carrying out the Chief Information Officer responsibilities and serve as the primary liaison to the Covered Entity's authorizing officials, information system owners, and information system security officers.

The CISO ensures that information resources and technologies are effectively protected and shall oversee the development, implementation, and enforcement of security policies. The CISO can work alongside the chief information officer in procuring cybersecurity products and services, and managing disaster recovery and business continuity plans.

SEC. 9. Covered Entity who rely on third-party owned CII. – Covered Entity remain responsible for the cybersecurity and resilience of the computer systems they rely on to deliver their respective mandates, even if those systems are managed by a third party. Covered Entity who depends on third-party-owned CII shall secure legally binding commitments from these vendors ensuring that the third party meets the cybersecurity standards and requirements applicable to CII, including incident reporting, auditing, and risk assessment.

SEC. 10. Data Privacy and Disclosure of Nonpublic Personal Information - All Covered Entities shall protect their client's right to privacy. In this regard, Covered Entities shall comply with the requirements of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012, its implementing rules and regulations, and other relevant rules that may be applicable to the protection of personal data, whether issued by the Commission or other government agencies.

SEC. 11. Information Sharing – Covered Entities shall comply with and integrate communication protocols in their respective cyber resilience framework to ensure that certain information is shared only to the desired and appropriate audience or recipient. The information sharing protocols adopted by Covered Entities shall be in accordance with international best practices and other relevant rules and regulations on information sharing, which the pertinent government agency having jurisdiction on the matter may from time to time issue.

SEC. 12. Cybersecurity Audit and Risk Assessment of Covered Entities. – Covered Entities shall regularly review their cyber resilience framework to ensure that they continue to be appropriate to manage adverse impacts of the cyber risks in their operations. All Covered Entities shall take the necessary steps to identify, assess, and institute technical or procedural controls to mitigate cybersecurity risks at least once every three (3) years.

At least once every two (2) years (or at such higher frequency as may be determined by the Commission in any particular case), all Covered Entities shall submit an authenticated cybersecurity audit and risk assessment report performed by a DICT recognized Cybersecurity Assessment

Provider. Cybersecurity audit and risk assessment reports shall be submitted to the Commission and shall be kept in record for a period of not less than five (5) years.

SEC. 13. Availability of Documents and Policies Relating to Cyber Resilience - Policies and documents pertinent to the implementation of the cyber resilience framework shall be made available by each Covered Entity to the Commission, in the event of audit or on-site examinations.

SEC. 14. Material Cyber Incident – A cyber incident shall be reported by the Covered Entities to the Commission, insofar as such incident is a material event which would reasonably be expected to materially affect the decision of investors to buy, to sell or to hold securities, which shall include but not limited to the following:

14.1. It creates a risk on the investments on any of the securities of the Covered Entity, or its investors, as the case may be,

14.2. Ten percent (10%) or more change in the financial condition or results of operation of the Covered Entity.

14.3. Any similar event that would reasonably be expected to affect the decision of the Covered Entity's investors.

SEC. 15. Mandatory Disclosure to the Commission – If a Covered Entity experiences a cyber incident that is determined to be material, the Covered Entity shall disclose to the Commission, through the Markets and Securities Regulation Department, the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the Covered Entity, including its financial condition and results of operation.

A Covered Entity shall disclose the cyber incident by filing a report to the Commission within five (5) days after the occurrence of the event. The report shall contain the following information and exhibits:

15.1. Name of the authorized person to submit the report;

15.2. Date when the incident was first detected;

15.3. Nature of the information security incident;

15.4. Possible business processes and functions compromised;

15.5. Market Participant's initial response and next steps; and

15.6. Risk assessment

15.7. Incident progress report

15.8. Post-incident report, which contains the following information:

15.8.1. the magnitude of business operations compromised;

15.8.2. the agency's response; and

15.8.3. mitigation strategy

SEC. 16. Supplemental Regulations – This circular may be supplemented by relevant regulations which the Commission may from time to time issue.

SEC. 17. Applicability of Certain Laws and Regulations – The provisions of the SRC and its implementing rules and regulations, and other relevant laws and regulations insofar as they are applicable and not inconsistent herewith, shall apply suppletorily. This circular shall be without prejudice to and shall be functionally equivalent to the other regulations on cybersecurity issued by the relevant government agencies.

SEC. 18. Administrative Sanctions – The Commission shall impose sanctions provided under the FCPA and the SRC and its respective implementing rules and regulation in case of violation of this circular.

SEC. 19. Transitory Provision - Covered Entities shall comply with the provisions of these Guidelines within at least one (1) year from the date of effectivity, considering the complexities of their respective information technology structures.

SEC. 20. Effectivity – This circular shall take effect fifteen (15) days after its complete publication in the *Official Gazette* or in at least two (2) newspapers of national circulation in the Philippines.

Done this _____ in Makati City, Philippines.

For the Commission:

FRANCISCO ED. LIM
Chairperson