



MEMORANDUM – 2020-035

TO : THE TRADING PARTICIPANTS AND THE INVESTING PUBLIC


SUBJECT : REQUEST FOR COMMENTS ON THE PROPOSED GUIDANCE FOR REGULATED ENTITIES ON ESTABLISHING AND MAINTAINING A CYBERSECURITY FRAMEWORK



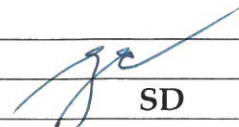
DATE : 17 DECEMBER 2020

The Securities and Exchange Commission (“Commission”) intends to issue a regulation for cybersecurity framework entitled “*Guidance for Regulated Entities on Establishing and Maintaining a Cybersecurity Framework*”. Thus, the Commission is inviting market participants, the investing public, and other interested parties to submit their views, comments, and inputs on the proposed rules.

A copy of the proposed rules is attached herewith for reference.

The comments may be addressed to the Markets and Securities Regulation Department (MSRD), Ground Floor, Secretariat Building, PICC Complex, Roxas Boulevard, Pasay City, c/o Ms. Sheryl Espiña and Ms. Gretchen Lagonoy **not later than 31 January 2021**. Alternatively, the comments may be sent via electronic mail to msrd_covid19@sec.gov.ph , mrd@sec.gov.ph , slespina@sec.gov.ph , and gclagonoy@sec.gov.ph .


DAISY P. ARCE
President

 ACD	 FHRAD	IED	 SD
--	--	-----	---



**SEC Memorandum Circular No. ____
Series of 2020**

TO : ALL CONCERNED, INCLUDING ALL CAPITAL MARKET-RELATED ENTITIES

SUBJECT : GUIDANCE FOR REGULATED ENTITIES ON ESTABLISHING AND MAINTAINING A CYBERSECURITY FRAMEWORK

DATE : 15 DECEMBER 2020

WHEREAS, the Securities and Exchange Commission (“Commission”) recognizes that cyber crime is currently the fastest rising economic crime, in line with the findings under the National Security Policy for 2017-2022

WHEREAS, the Philippine Government promotes to pursue and advance Informational and Cybersecurity as one of its 12-point National Security Agenda, where it endeavors to shield the country from computer-generated/cyber-attacks that could cause massive crises in our economy, banking and financial institutions, communications and other critical infrastructures.

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, the framework for cybersecurity must be institutionalized consistent with the guidelines set forth by the Board of the International Organization of Securities Commission, and must principally be implemented among financial markets in the Philippines;

WHEREAS, this regulation adopts the concepts of Cybersecurity and Cybercrime as stated in the National Cybersecurity Plan 2022, the Cybercrime Prevention Act of 2012 and its corresponding implementing rules and regulations.

WHEREAS, the Commission recognizes that regulatory approaches tend to be high-level and allow for flexibility, recognizing that there is no “one size fits all” approach that market participants should adopt.

WHEREFORE, IN VIEW OF THE FOREGOING, the Commission shall require all securities markets participants to comply with the following guidelines:

SEC. 1. Scope – these guidelines shall apply to all securities markets participants, which shall refer to a broad range of participants, entities, and securities and derivatives markets that include trading venues, Trading Participants such as broker-dealers, asset managers, Transfer Agents, Self-Regulatory Organizations, and such other regulated entities with a secondary license issued by the Commission. For brevity, the foregoing entities shall be collectively referred under these rules as “Regulated Entities.”

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

- 2.1. **Cyber attacks** – refers to attempts to compromise the confidentiality, integrity and availability of computer data or systems.
- 2.2. **Cyber risks** – refers to the potential negative outcomes associated with cyber attacks.
- 2.3. **Cybersecurity** – refers to all of the important activities associated with mitigating cyber risk, namely to identify, protect, detect, respond, and recover from cyber attacks. It shall likewise encompass protection of investor and firm information from compromise through the use—in whole or in part—of electronic digital media (e.g., computers, mobile devices or Internet protocol-based telephony systems).
- 2.4. **Incident Response Plan** – refers to a written plan that embodies a systematic approach taken by a securities markets to respond to and manage a cyber attack.
- 2.5. **Insider trading** – refers to the act of an insider in selling or buying a security of the issuer, while in possession of material information in respect to the issuer or the security that is not generally available to the public. The definition provided under Sec. 27 of the SRC shall be adopted for purposes of implementing this circular.
- 2.6. **Issuer** – is an entity authorized by the Commission to offer to sell, sell or promote the sale to the public of its equity, bonds, instruments of indebtedness and other forms of securities.
- 2.7. **Securities Market Participants** – refers to a range of participants, entities, and securities and derivatives markets that include trading venues, Trading Participants such as broker-dealers, asset managers, Transfer Agents, Self-Regulatory Organizations, and such other regulated entities with a secondary license issued by the Commission.
- 2.8. **Trading venue** – means exchanges or other multilateral trading facilities, including, for example, alternative trading systems (ATs) and multi-lateral trading facilities (MTFs). It also refers to the operator of a particular exchange or trading facility

CHAPTER I.
COMMON PROVISIONS

A. CYBERSECURITY GOVERNANCE

SEC. 1. Practices required from Regulated Entities to reinforce cybersecurity – The following practices must be incorporated by Regulated Entities in dealing with cyber security risks:

1.1. Identification – Regulated Entities must consider cyber security to be an integral part of the enterprise risk management program, which must include the identification of critical assets, information and systems, including order routing systems, risk management systems, execution systems, data dissemination systems and surveillance systems.

- i.** Regulated Entities must involve its senior management and company boards in determining their risk appetite and priorities and allocating resources to cyber security.
- ii.** To augment their identification of cyber security issues, Regulated Entities must also adopt the establishment and maintenance of an inventory of all authorized and non-authorized hardware and software, and likewise undertake third-party and technology providers' security assessments.

1.2. Protection – Regulated Entities must adopt organizational or technical measures to strengthen cybersecurity including, but not limited to:

- i.** Risk assessments to determine the minimum level of controls to be implemented within a project, an application or a database,
- ii.** Employee training and awareness initiatives,
- iii.** Operation of segregated platforms for trading systems and web services in order to prevent contagion.

1.3. Detection – Regulated Entities must maintain external and internal monitoring of traffic and logs to detect abnormal patterns of access and other anomalies.

1.4. Response – Regulated Entities must develop a formalized Incident Response Plan (“IRP”), which must be regularly practiced and updated, to address any breach of cybersecurity. The response plans to be implemented by Regulated Entities must include the following:

- i.** Preparing communication/notification plans for informing relevant stakeholders,

- ii. Conducting forensic analysis to understand the anatomy of a breach or an attack,
- iii. Maintaining a database recording cyber attacks,
- iv. Conducting cyber drills, firm-specific simulation exercises as well as industry-wide scenario exercise.

1.5. Recovery – Regulated Entities must develop a Disaster Recovery Plan and a Business Continuity Plan, which incorporates significant components of operational risk management, and includes policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption.

B. INFORMATION SECURITY MANAGEMENT

SEC. 1. Creation. – Regulated Entities must endeavor to establish an Information Security Group (“InfoSec”) that is separate and distinct from its existing Information Technology group. The primary focus of the InfoSec team is to ensure the confidentiality, integrity, and availability of information in the processes of the Regulated Entity.

SEC. 2. Senior Officer Appointment. A suitable senior officer such as a Chief Information Security Officer (CISO) should be appointed to oversee the InfoSec Group and the entire cybersecurity framework of the Regulated Entity and shall have the responsibility of liaising with the Senior Management following best practices and staying current with all related technologies, and cybersecurity trend.

- 2.1. The appointed CISO should be suitably qualified, experienced and have a good understanding and knowledge of Information Technology (IT) systems and cybersecurity.
- 2.2. The CISO should be provided with sufficient delegated operational authority to carry out his or her role.

SEC. 3. Responsibilities. – The InfoSec Group is in-charge to implement and execute the following functions and strategies:

- 3.1. **Planning** – The CISO shall coordinate with appropriate security managers to develop an operational security plan with the goal of supporting the long-term achievement of the overall organizational strategy. The Regulated Entity’s InfoSec plan must strive to cover critical areas, such as but not limited to:
 - i. Incident Response Planning;
 - ii. Business Continuity Planning;
 - iii. Disaster Recovery Planning;
 - iv. Policy Planning;
 - v. Personnel Planning;
 - vi. Technology Rollout Planning;

- vii. Risk Management Planning; and
- viii. Security Program Planning

3.2. Policy – The InfoSec Group shall draft guidelines that will dictate certain behavior within the organization pertaining to handling cybersecurity. The following policies must be drafted and implemented in the entire organization of the Regulated Entity:

- i. **Enterprise Information Security Policy** – Developed within the context of the Strategic Information Technology Plan, this sets the tone for the InfoSec Group and the InfoSec climate across the organization.
- ii. **Issue-Specific Security Policies** – These are sets of rules that define acceptable behavior within a specific organization resource, such as e-mail or Internet usage.
- iii. **System-Specific Policies** – A merger of technical and managerial intent, System-Specific Policies include both the managerial guidance for the implementation of a technology as well as the technical specifications for its configuration.

The Regulated Entities shall submit the foregoing policies to the Commission within one (1) year from the enactment of this Circular and in such instances when substantial modification has been introduced thereto.

3.3. Programs – The following programs, in relation to Sec. 3.1 of this Chapter, shall be implemented by the InfoSec Group:

- i. Employee Security Education, Training and Awareness Program
- ii. Risk Management Program
- iii. Contingency Programs

SEC. 4. Cybersecurity Workforce Assessment – The InfoSec Group shall be primarily responsible in developing a comprehensive workforce strategy to enhance the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Regulated Entity.

4.1. Employee Selection. – An effective screening process with stringent selection criteria should be implemented by the Regulated Entities that is comprehensive and effective to assure careful selection of staff, vendors and contractors who support technology functions and to minimize cyber risks due to system failure, internal sabotage or fraud.

4.2. Training and Awareness. - Regulated entities should have a formalized plan to provide ongoing technical training to their cybersecurity personnel and IT unit/team (including those involved in developing, maintaining and operating websites and systems) on IT systems and current and emerging cybersecurity subject areas as well as security principles to ensure they are knowledgeable and aptly trained for their specific IT or cybersecurity roles and functions.

4.3. Communication to Senior Management. - Regulated entities should ensure cybersecurity policies and procedures are communicated to senior management and staff at all levels and training is conducted on regular basis.

SEC. 5. Risk Management. - The InfoSec Group's implemented cybersecurity risk management strategy should involve putting measures in place to ensure the confidentiality, integrity and availability of their data and systems.

5.1. Key functions to manage cybersecurity risk. - In line with the practices set forth in Chapter I, A, Sec. 1 of this rule, Regulated Entities must adhere to the following core functions to address its dynamic cybersecurity risk:

- i. Identify** - developing an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The Regulated Entity must be able to understand the business context, the resources that support critical functions, and the related cybersecurity risks in order to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
- ii. Protect** - developing and implementing appropriate safeguards to ensure delivery of critical services. This function is critical for Regulated Entities to support the ability to limit or contain the impact of a potential cybersecurity event.
- iii. Detect** - developing and implementing appropriate activities to promptly identify the occurrence of a cybersecurity event.
- iv. Respond** - developing and implementing appropriate activities to take action regarding a detected cybersecurity incident and supports the ability to contain the impact of a potential cybersecurity incident.
- v. Recover** - Developing and implementing appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. This function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

SEC. 6. Contingency Planning. - Regulated Entities must be able to provide steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency.

6.1. Cyber Incident Response - It is imperative for the InfoSec Group to come up with a *Cyber Incident Response Plan* which focuses on detection, response, and recovery to a computer security incident or event, that may be embodied in the following plans:

- i. Business Impact Analysis** – Refers to an analysis of an information system’s requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. The purpose of the BIA is to identify and prioritize system components by correlating them to the mission/business process(es) the system supports, and using this information to characterize the impact on the process(es) if the system were unavailable.
 - ii. Cyber Incident Response Plan** – The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attacks against an organization’s information system(s). The cyber incident response plan establishes procedures to address cyber-attacks against an organization’s information system. These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software, or data.
 - iii. Disaster Recovery Plan (DRP)** – This refers to a written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. The DRP applies to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period. A DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency. This plan only addresses information system disruptions that require relocation.
 - iv. Business Continuity Plan (BCP)** – The documentation of a predetermined set of instructions or procedures that describe how an organization’s mission/business processes will be sustained during and after a significant disruption. The InfoSec Group must coordinate with information system owners to ensure that the BCP expectations and Information Systems capabilities are matched.
- 6.2. Contingency Planning Process.** – The following steps represent key elements that must be observed by a Regulated Entities’ InfoSec Group in the event of a cyber-attack:
- i. Develop the contingency planning policy** - The contingency planning policy statement should define the organization’s overall contingency objectives and establish the organizational framework and responsibilities for system contingency planning.

- ii. **Conduct the Business Impact Analysis** - The BIA characterizes the system components, supported mission/business processes, and interdependencies. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the Regulated Entities' BCP and DRP.
- iii. **Identify preventive controls** - In some cases, the outage impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, and/or reduce impacts to the system. Where feasible and cost-effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption.
- iv. **Create contingency strategies** - Contingency strategies are created to mitigate the risks for the contingency planning family of controls and cover the full range of backup, recovery, contingency planning, testing, and ongoing maintenance.
- v. **Develop an information system contingency plan (ISCP)** - The plan contains detailed roles, responsibilities, teams, and procedures associated with restoring an information system following a disruption. The ISCP should document technical capabilities designed to support contingency operations and should be tailored to the organization and its requirements.
- vi. **Ensure plan testing, training, and exercises (TT&E)** - Organizations should conduct TT&E events periodically, following organizational or system changes, or the issuance of new TT&E guidance, or as otherwise needed. Execution of TT&E events assists organizations in determining the plan's effectiveness, and that all personnel know what their roles are in the conduct of each information system plan.
- vii. **Ensure plan maintenance** - To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. As a general rule, the plan should be reviewed for accuracy and completeness at an organization-defined frequency or whenever significant changes occur to any element of the plan.

C. DATA PROTECTION

SEC. 1. Data privacy and disclosure of nonpublic personal information - It is the policy of the Commission that all Regulated Entities have an affirmative and continuing obligation to respect the privacy of its clients and to protect the security and confidentiality of those clients' nonpublic personal information.

1.1. Data Protection. – Regulated entities should implement policies, procedures, internal control mechanisms and training that:

- i. support the protection of privacy of clients’ personal information and sensitive personal information including preventing or minimizing the misuse or inappropriate communication of personal information to third parties; and
- ii. assess the cyber risks that may result in a failure to protect the privacy of personal information including any exposures relating to the use of third-party providers.

1.2. Notification for failure to protect privacy. Regulated entities should establish suitable response measures where a failure to protect the privacy of personal information occurs, including matters such as timely notification to affected clients and relevant competent authorities.

1.3. Disclosure of Institution Privacy Policy to clients of SROs and other entities with secondary license issued by the Commission, and stakeholders of Publicly Listed Companies. - At the time of establishing a customer relationship with a client and not less than annually during the continuation of such relationship, a Regulated Entity shall provide a clear and conspicuous disclosure to such client, in writing or in electronic form or other form permitted by pertinent regulations, of such participant’s policies and practices with respect to—

- i. disclosing nonpublic personal information to affiliates and nonaffiliated third parties, including the categories of information that may be disclosed;
- ii. disclosing nonpublic personal information of persons who have ceased to be customers of the financial institution; and
- iii. protecting the nonpublic personal information of its clients and stakeholders.

1.4. Information to be included – The disclosure required by Sec. 2.1 shall include –

- i. the policies and practices of the institution with respect to disclosing nonpublic personal information to nonaffiliated third parties;
- ii. the categories of nonpublic personal information that are collected by the Regulated Entity;
- iii. the policies that the Regulated Entity maintains to protect the confidentiality and security of nonpublic personal information; and

- iv. such other required disclosures under relevant rules and regulations.

D. REVIEW OF THE CYBERSECURITY FRAMEWORK

SEC.1. Regular review of cybersecurity Framework. – Regulated entities should regularly review the cybersecurity arena and information technology space and assess their cybersecurity framework to ensure they continue to be appropriate to manage adverse impacts of the cyber risks and IT risks on the regulated entities' business.

SEC. 2. Transparency of implementation of cybersecurity framework. – The cybersecurity framework should include a "feedback loop" which ensures transparency and allows the Senior Management to take necessary action in response to changes in the cybersecurity risk profile of Regulated Entities, particularly between the InfoSec and the designated. The feedback loop will also ensure that decisions made by the Regulated Entities' InfoSec Group and Senior Management are implemented and their effects monitored to determine whether they are in fact appropriate.

SEC. 3. Report to the Commission. – The Commission may require Regulated Entities to submit a sworn documentation from its InfoSec Group and/or Senior Management to ensure compliance with the regular review of the cybersecurity framework, in such frequency as may be deemed necessary.

E. ACCOUNTABILITY

SEC. 1. Joint responsibilities and accountability of the InfoSec Group and the Senior Management. - The InfoSec and Senior Management's duties and responsibilities relating to cybersecurity should include, but not be limited to:

- 1.1. Ensuring that a sound and robust cybersecurity framework is established and maintained and have accountability and ownership of the framework and the financial resources for the framework. They should also be involved in key IT decisions.
- 1.2. Approving appropriate programs, policies and procedures for cybersecurity, cyber-resilience and IT management.
- 1.3. Ensuring that effective internal controls and cybersecurity risk management practices are implemented to achieve on-going security, reliability, resiliency and recoverability.
- 1.4. Properly assessing cost-benefit issues, including factors such as reputation, customer confidence, consequential impact and legal implications, regarding investment in controls and security measures for computer systems, networks, data centres, operations and backup facilities. The costs associated with managing cybersecurity risks should be balanced against resulting benefits while maintaining operational and financial stability.

- 1.5. Ensuring that management supports the senior officer accountable for cyber-resilience by the creation, implementation, testing and ongoing improvement of cyber-resilience plans, which are appropriately harmonized across the business.
- 1.6. Ensuring that a formal, independent cybersecurity and cyber-resilience review/audit of the organization is carried out, at a minimum, annually.

SEC. 2. Accountability of the InfoSec Group. -

- 2.1. Establishing a well-documented comprehensive cybersecurity training program for the InfoSec to help ensure it has the requisite knowledge to competently exercise its oversight function and assess the adequacy and effectiveness of the overall cyber resilience program.
- 2.2. Overseeing cybersecurity and cyber-resilience. The InfoSec Group may, as necessary, delegate primary oversight activity to an existing committee (e.g. the risk committee) or a new committee (e.g. a cyber-resilience committee).
- 2.3. Having a good command of cyber risks and the cybersecurity environment including regular training in this regard. InfoSec staff should receive orientation on joining the entity and receive regular updates on recent threats and trends.
- 2.4. Holding management accountable for reporting a quantified and comprehensible assessment of cyber risks, threats and events as a standing agenda item during its meetings.
- 2.5. Ensuring that one Senior officer is appointed who is accountable for reporting on the organization's capability to manage the implementation of the cybersecurity framework and cyber-resilience program. The InfoSec Group should ensure that this officer has regular access to the InfoSec Group processes, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.
- 2.6. Ensuring that management integrates cyber resilience and cyber risk assessment into the overall business strategy and enterprise-wide risk management, as well as budgeting and resource allocation.
- 2.7. Annually defining and quantifying the business risk tolerance relative to cybersecurity and cyber-resilience and ensuring that this is consistent with the strategy and risk appetite.
- 2.8. Carrying out periodic reviews of its own performance in the implementation of the cybersecurity framework and cyber resilience and/or seeking independent advice for continuous improvement, if necessary.

SEC. 3. Accountability of the Senior management –

- 3.1.** Developing, implementing and monitoring the cybersecurity framework by documenting appropriate policies and procedures and controls relating to cybersecurity, cyber-resilience and IT system controls.
- 3.2.** Ensuring that there is clear and ready communication to keep the InfoSec Group apprised of the Regulated Entity’s potential cyber-risks, current threats, incidents or attacks that are deemed material as well as any necessary changes to the regulated entity’s cybersecurity framework and IT systems.

CHAPTER II. **PUBLICLY LISTED COMPANIES**

SEC. 1. Disclosures required – Publicly listed companies must make a full, accurate, and timely disclosure of financial results, risk and other information which is material to investors’ decisions. Issuers who have experienced cybersecurity breach and those subject to material cybersecurity risk but may not yet have been the target of a cyber-attack, must promptly take all required actions to inform investors about material cybersecurity risks.

- 1.1.** The following risk factors must be disclosed by PLCs in its registration statement:
 - i.** reasons why the issuer is subject to cyber risk;
 - ii.** the source and nature of the cyber risk, and how the risk may materialize;
 - iii.** the possible outcomes of a cyber incident, for example:
 - a.** effects on the issuer’s reputation and customer confidence;
 - b.** effects on stakeholders and other third-parties;
 - c.** costs of remediation after a breach;
 - d.** litigation, whether brought by parties seeking damages against the issuer or by the issuer against third parties, including regulatory investigation, and remediation costs associated with cybersecurity incidents;
 - e.** effects on the issuer’s internal and disclosure controls;
 - iv.** the adequacy of preventive measures and management’s strategy for mitigating cyber risk, which must include the following factors as integral parts of an existing risk management program:
 - a.** the nature of the board’s role in overseeing the management and identification of that risk;
 - b.** organizational or technical measures in enhancing their cyber security;

- c. implemented procedures in the detection of abnormal patterns of access and other anomalies;
 - d. the company's response plan for those types of incidents to which it is most likely to be subject;
 - e. a recovery plan enforced in order to restore any capabilities or services that were impaired.
- v. whether a material breach has occurred previously and how this affects the issuer's overall cyber risk;
 - vi. the probability of the occurrence and potential magnitude of cybersecurity incidents;
 - vii. such other material cybersecurity risks or incidents that will significantly compromise information or the business and scope of company operations.
- 1.2. The following items must be considered by the PLC in their Management Discussion and Analysis:
- i. Cost of ongoing cybersecurity efforts;
 - ii. Costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents, among other matters;
 - iii. Such other array of costs associated with cybersecurity issues, including, but not limited to:
 - a. loss of intellectual property,
 - b. the immediate costs of the incident,
 - c. costs associated with implementing preventive measures,
 - d. maintaining insurance,
 - e. responding to litigation and regulatory investigations,
 - f. preparing for and complying with proposed or current legislation,
 - g. engaging in remediation efforts,
 - h. addressing harm to reputation, and
 - i. loss of competitive advantage that may result.
- 1.3. Companies are required to file the required periodic reports to disclose specified information on a regular and ongoing basis. In doing so, companies must always reduce the risk of selective disclosure in their reports. An ongoing internal or external investigation would not, on its own, provide a basis for avoiding disclosures of a material cybersecurity incident.

SEC. 2. Insider Trading – Companies and their directors, officers, and other corporate insiders should be mindful of complying with the laws related to insider trading in connection with information about cybersecurity risks and incidents, including vulnerabilities and breaches.

CHAPTER III.
SELF-REGULATORY ORGANIZATIONS AND OTHER ENTITIES WITH SEC SECONDARY LICENSE

SEC. 1. Scope – This chapter shall specifically apply to Brokers and Dealers, Exchanges, Transfer Agents, Clearing Agencies and Securities Depositories, Self-Regulatory Organization, and such other entities with Secondary License issued by the Commission.

SEC. 2. Responsibility of Covered Entities – Entities covered under this Chapter must work together with the Commission in order to foster a safer electronic trading environment that aims to protect investor privacy, confidential information and other important trading aspects by strengthening the trading systems' infrastructure.

SEC. 2. Requirements for Registration – Every application for registration with the Commission of the entities mentioned in Sec. 1 of this Chapter shall be accompanied by a Comprehensive Information Technology Plan, to include among others: a) a list and brief description of the software and hardware to be primarily used in its functions and their location; b) a back-up system or subsystem and their location; c) security system and procedures to be employed; d) procedures to check sufficiency of system's capacity and expansion program, if necessary; and e) IT system maintenance schedule.

SEC. 3. Audit of Information Technology Systems – Entities covered under this chapter shall subject their information technology, business continuity and disaster recovery, and risk management systems to a regular review and audit by an independent firm at least once every three (3) years and such other frequency that the Commission may deem necessary. The results of the said review and audit shall be submitted to the Commission within thirty (30) days from completion of the audit.

SEC. 4. Report to the Commission – Entities with SEC Secondary License shall report to the Commission any disruption, business continuity activation, or any other event that could affect the integrity of its cybersecurity framework. The report shall include the steps take, and/or to be taken to remedy the situation, which must be submitted to the Commission not later than five (5) days from the occurrence of such event.

CHAPTER IV.
MISCELLANEOUS PROVISIONS

SEC. 1. Supplemental Regulations – This circular may be supplemented by relevant regulations which the Commission may from time to time issue.

SEC. 2. 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 hereto.

SEC. 3. Administrative Sanctions – If the Commission finds that there is a violation of any provision of this circular or any applicable rules under the SRC, or that any person, in a registration statement or its supporting papers and the prospectus, as well as in the periodic reports required to be filed with the Commission has made any untrue statement of a material fact or omitted to state

any material fact required to be stated therein or necessary to make the statements therein not misleading or refuses to permit any lawful examination into its corporate affairs, the Commission shall, in its discretion impose additional sanctions provided by law aside from those established by existing regulations.

SEC. 4. 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 general circulation in the Philippines.

Pasay City, Metro Manila, _____ 2020.

EMILIO B. AQUINO
Chairperson