THE PHILIPPINE STOCK EXCHANGE, INC.
& Subsidiaries

ENTERPRISE RISK MANAGEMENT FRAMEWORK

2021

TABLE OF CONTENTS

ANNEXES

VERSION HISTORY

Version	Date	Reason for Revision	No. of Pages Revised	Prepared by	Approved by
1.0	July 30, 2021	Creation of a new ERM framework	n/a	**Meyrick A. Cello** *Risk Officer*	**PSE Board of Directors** **PSE Risk Management Committee** **Ramon S. Monzon** *President/CEO* **Roel A. Refran** *COO/CRO*

PREFACE

At the enterprise level, risk management is about achieving strategic objectives and creating value, all while ensuring that the key activities undertaken are neither too risky nor too conservative to achieve the stated outcomes. In everyday operations, this means that the outcome, or result, of any strategic objective is uncertain until the result or achievement of the objective becomes a reality or an accomplishment, or results in a loss event, incident, or crisis.

OBJECTIVES OF ENTERPRISE RISK MANAGEMENT

In line with the main public policy objectives of the Committee on Payment and Settlement Systems ("CPSS") and the Technical Committee of the International Organization of Securities Commissions ("IOSCO"), the objective of the Enterprise Risk Management ("ERM") framework is to provide guidance on adequately preventing and managing systemic crises and other key risks[1], which could result in financial shocks when passed from one participant or financial market infrastructure ("FMI") to another. The effects of such a disruption could extend well beyond the FMIs and market participants, threatening the stability of domestic and international financial markets and the broader economy. The Philippine Stock Exchange, Inc. ("PSE" or the "Exchange") strives to strengthen its position as a robust and efficient FMI in the Philippine financial market, giving participants the confidence to fulfill their obligations on time, even in periods of market stress.[2] The Securities Clearing Corporation of the Philippines ("SCCP"), as a central counterparty to all trades in the PSE, ensures the finality of trade transactions.

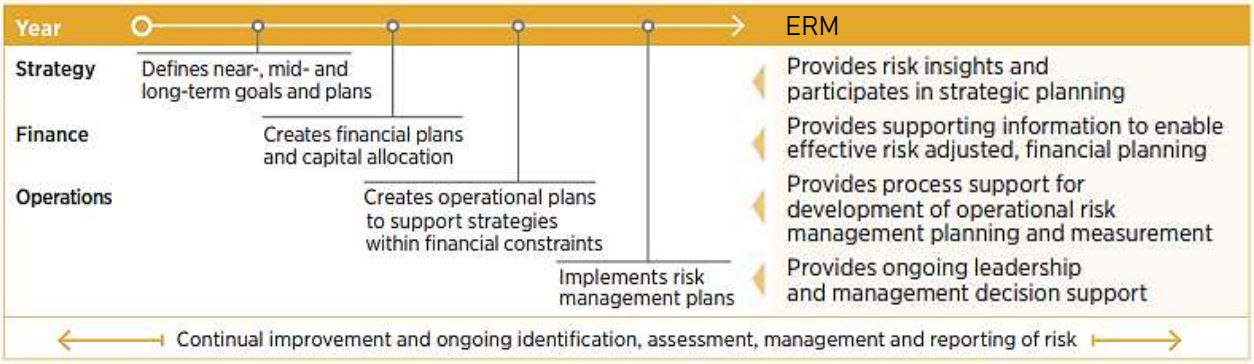
The purpose of the ERM framework is to assist the Exchange (the "Parent") and its subsidiaries, SCCP and Premier Software Enterprise, Inc. ("PSEI") (the "Group") in integrating risk management into significant activities and functions to achieve their strategic and business objectives. The effectiveness of risk management shall depend on its integration into the governance and decision-making activities of the Group, down to management of trading participants ("TPs")[3] and critical third-party service providers. The implementation of the ERM framework shall require support from stakeholders, particularly top management and the Board of Directors.[4]

[1] Refer to **Annex H** for the *Key Risk Areas.*
[2] IOSCO PD377 *Section 1.15. Public Policy Objectives.*
[3] PSE *Revised Trading Rules* (June 2010): An entity authorized by the Exchange to own and operate a trading right, pursuant to the Exchange By-laws and applicable rules.
[4] ISO 31000 *Section 4: Principles.*

SCOPE & APPLICABILITY OF THE FRAMEWORK

This framework highlights the integration of enterprise risk management into all aspects of the Group's operations starting with the integration into the strategy-setting process, the setting of business objectives, and managing risk in execution, wherein the consideration of risk is not positioned as an additional or separate activity. The importance and role of ERM is presented through the lens of supporting the Group's operations, managing performance, and ultimately creating, realizing, and preserving value. The framework does not refer to solely reporting risk, but also on the reporting of potential or actual manifestations of risk impacting performance and the achievement of strategy and business objectives. We note that this framework is designed to integrate ERM as part of the management and operations of the Group, as opposed to a distinct or siloed activity.

Figure 1. Integration of ERM into the Strategic and Operational Cycle*



*WBCSD & COSO (October 2018) *Enterprise Risk Management: Applying enterprise risk management to environmental, social and governance-related risks. Figure 1.1.*

ABBREVIATIONS

BIS	Bank for International Settlements
BOD	Board of Directors
BSP	Bangko Sentral ng Pilipinas
CMIC	Capital Markets Integrity Corporation
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPSS	Committee on Payment and Settlement Systems
ERM	Enterprise Risk Management
ESG	Environmental, Social, and Governance
FMI	Financial Market Infrastructure
GPC	Governance Professionals of Canada
IOSCO	International Organization of Securities Commissions
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	Information Technology
LOD	Line of Defense
MkSE	Makati Stock Exchange
MSE	Manila Stock Exchange
NOMELEC	Nominations and Elections Committee
PDSHC	Philippine Dealing System Holdings Corporation
PSE	The Philippine Stock Exchange, Inc.
RMC	Risk Management Committee
SCCP	Securities Clearing Corporation of the Philippines
SEC	Securities and Exchange Commission
SRC	Securities Regulation Code
SSS	Securities Settlement System
TP	Trading Participant
WBCSD	World Business Council for Sustainable Development
WFE	World Federation of Exchanges

TERMINOLOGIES & DEFINITIONS

Business Continuity	A state of uninterrupted business operations. This term also refers to all of the organizational, technical, and staffing measures used to ensure the continuation of operations following a disruption to a service, including in the event of a wide-scale or major disruption. [IOSCO PD377]
Central Counterparty	An entity that interposes itself between counterparties to contracts traded in one or more financial markets, becoming the buyer to every seller and the seller to every buyer and thereby ensuring the performance of open contracts. [IOSCO PD377]
Central Securities Depository	An entity that provides securities accounts, central safekeeping services, and asset services, which may include the administration of corporate actions and redemptions, and plays an important role in helping to ensure the integrity of securities issues (that is, ensure that securities are not accidentally or fraudulently created or destroyed or their details changed). [IOSCO PD377]
Clearing Fund	A prefunded default arrangement that is composed of assets contributed by a CCP's participants that may be used by the CCP in certain circumstances to cover losses or liquidity pressures resulting from participant defaults. [IOSCO PD377]
Collateral	An asset or third-party commitment that is used by a collateral provider to secure an obligation vis-à-vis a collateral taker. [IOSCO PD377]
Compliance Risk	Compliance risk is the threat posed to a company's financial, organizational, or reputational standing resulting from violations of laws, regulations, codes of conduct, or organizational standards of practice. [Deloitte]
Core Values	The entity's beliefs and ideals about what is good or bad, acceptable or unacceptable, which influence the behavior of the organization. [COSO 2017]
Counterparty	A party to a trade. [IOSCO PD377]
Credit Risk	The risk that a counterparty, whether a participant or other entity, will be unable to meet fully its financial obligations when due, or at any time in the future. Types of credit risk includes: replacement cost risk and principal risk. [IOSCO PD377]
Culture	The attitudes, behaviors, and understanding about risk, both positive and negative, which influence the decisions of Management and personnel and reflect the mission, vision, and core values of the organization. [COSO 2017]

Current Exposure	The loss that an FMI (or in some cases, its participants) would face immediately if a participant were to default. Current exposure is technically defined as the larger of zero or the market value (or replacement cost) of a transaction or portfolio of transactions within a netting set with a counterparty that would be lost upon the default of the counterparty. [IOSCO PD377]
Current Exposure	The loss that an FMI (or in some cases, its participants) would face immediately if a participant were to default. [IOSCO PD377]
Custody Risk	The risk of loss on assets held in custody in the event of a custodian's (or subcustodian's) insolvency, negligence, fraud, poor administration, or inadequate record-keeping. [IOSCO PD377]
Cyber Security Risk	Cyber security risk is the risk of exposure to a harmful activity, executed by one group or individual through computers, IT systems, and/or the internet, and targeting the computers, IT infrastructure, and internet presence of another entity. [IOSCO PD146] The realization of cyber security risk typically involves unauthorized access and/or unauthorized use of information and communications technology. [COSO 2017]
Default	An event stipulated in an agreement as constituting a default. Generally, such events relate to a failure to complete a transfer of funds or securities in accordance with the terms and rules of the system in question. [IOSCO PD377]
Deferred Net Settlement	A net settlement mechanism which settles on a net basis at the end of a predefined settlement cycle. [IOSCO PD377]
Delivery Versus Payment	A securities settlement mechanism that links a securities transfer and a funds transfer in such a way as to ensure that delivery occurs if and only if the corresponding payment occurs. [IOSCO PD377]
Emerging Risks	Risks that have not yet been recognized or if they have been recognized, they are not well defined or understood. [COSO 2017]
Enterprise Risk Management	It is the organizational culture, capabilities, and practices integrated with strategy-setting and applied when carrying out strategies, with the purpose of managing risks in creating, preserving, and realizing value. ERM focuses on managing risk through: • Recognizing culture • Developing capabilities • Applying practices • Integrating with strategy setting and performance • Managing risk to strategy and business objectives • Linking to value [COSO 2017]

Environmental Risk	Climate change, natural resources, pollution and waste, and environmental opportunities. The contribution an entity makes to climate change through greenhouse gas emissions, along with waste management and energy efficiency. [COSO 2017]
ESG Risks	ESG-related risks are the environmental, social, and governance-related risks and/or opportunities that may impact an entity. [COSO 2017] Refer to definitions on *environmental risk*, *social risks*, and *governance*.
Final Settlement	The irrevocable and unconditional transfer of an asset or financial instrument, or the discharge of an obligation by the FMI or its participants in accordance with the terms of the underlying contract. Final settlement is a legally defined moment. [IOSCO PD377]
Financial Market Infrastructure	A multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions. [IOSCO PD377]
Fraud Risk	Fraud risk is the risk of exposure to any intentional act or omission designed to deceive, resulting in the suffering of a loss and/or the perpetrator achieving a gain. [COSO 2017]
Funding Liquidity Risk	The risk that a counterparty, whether a participant or other entity, will have insufficient funds to meet its financial obligations as and when expected, although it may be able to do so in the future. [IOSCO PD377]
General Business Risk	Any potential impairment of the FMI's financial position (as a business concern) as a consequence of a decline in its revenues or an increase in its expenses, such that expenses exceed revenues and result in a loss that must be charged against capital. [IOSCO PD377]
Governance	Governance is the set of relationships among an FMI's owners, Board of Directors (or equivalent), Management, and other relevant parties, including participants, authorities, and other stakeholders (such as participants' customers, other interdependent FMIs, and the broader market). [IOSCO PD377] It is a set of rules or principles defining rights, responsibilities and expectations between different stakeholders in the governance of corporations. A well-defined corporate governance system can be used to balance or align interests between stakeholders and can work as a tool to support a company's long-term strategy. [COSO 2017]
Human Capital	The knowledge, skills, competencies, and other attributes embodied in individuals that are relevant to economic activity. [COSO 2017]

Impact	The result or effect of a risk. There may be a range of possible impacts associated with a risk. The impact of a risk may be positive or negative relative to the entity's strategy or business objectives. [COSO 2017]
Information Security Risk	The enterprise discipline that protects information against disclosure to unauthorized users (ensuring confidentiality), improper modification (ensuring integrity), and non-access, when required (ensuring availability). [COSO 2017] It is the risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. [NIST]
Inherent Risk	The risk to an entity in the absence of any direct or focused actions by Management to alter its severity. [COSO 2017]
Investment Risk	Investment risk is the risk of loss faced by an FMI when it invests its own or its participants' resources, such as collateral. [IOSCO PD377]
Legal/ Regulatory Risk	The risk of the unexpected application of a law or regulation, usually resulting in a loss. [IOSCO PD377]
Liquidity	The level of rapidity or swiftness with which an asset, financial commodity, or security can be either bought or sold in the market for its market price. [Corporate Finance Institute]
Mark to Market	The practice of revaluing securities and financial instruments using current market prices. [IOSCO PD377]
Market Liquidity Risk	The liquidity risk in trading arising from the characteristics of the market, such as atomicity of participants, free entry and exit at no cost, and transparent information. [BIS]
Market Risk	Market risk involves the risk that prices or rates will adversely change due to economic forces. Such risks include adverse effects of movements in equity and interest rate markets, currency exchange rates, and commodity prices. Market risk can also include the risks associated with the cost of borrowing securities, dividend risk, and correlation risk. [US Federal Reserve]
Natural Capital	The stock of renewable and non-renewable natural resources (e.g., plants, animals, air, water, soils, minerals) that combine to yield a flow of benefits to people. [COSO 2017]
Netting	The offsetting of obligations between or among participants in the netting arrangement, thereby reducing the number and value of payments or deliveries needed to settle a set of transactions. [IOSCO PD377]

Novation	A process through which the original obligation between a buyer and a seller is discharged through the substitution of the CCP as seller to the buyer and buyer to the seller, creating two new contracts. [IOSCO PD377]
Operational Risk	The risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by an FMI. [IOSCO PD377]
Organizational Sustainability	The ability of an entity to withstand the impact of large-scale events. [COSO 2017]
People Risk	People risk can be defined as the risk that people do not follow the organization's procedures, practices and/or rules, thus deviating from expected behavior in a way that could damage the business's performance and reputation. [IOR]
Physical Delivery	Delivery of an asset, such as an instrument or a commodity, in physical form. [IOSCO PD377]
Potential Future Exposure	Any potential credit exposure that an FMI could face at a future point in time. Potential future exposure is technically defined as the maximum exposure estimated to occur at a future point in time at a high level of statistical confidence. Potential future exposure arises from potential fluctuations in the market value of a participant's open positions between the time they are incurred or reset to the current market price, and the time they are liquidated or effectively hedged. [IOSCO PD377]
Principal Risk	Often associated with settlement risk, principal risk is the risk that a counterparty will lose the full value involved in a transaction, for example, the risk that a seller of a financial asset will irrevocably deliver the asset but not receive payment. [IOSCO PD377]
Project Risk	Project risk represents the exposure of stakeholders to the implications of variations in project outcome, both positive and negative. It is an important component of strategic decision-making, program and portfolio management, and project governance, where investments are sanctioned or cancelled, and priorities are set. [PMI]
Replacement Cost Risk	Often associated with pre-settlement risk, replacement cost risk is the risk of loss of unrealized gains on unsettled transactions with a counterparty, e.g., unsettled transactions of a CCP. The resulting exposure is the cost of replacing the original transaction at current market prices. [IOSCO PD377]

Reputational Risk	Reputational risk is the risk arising from negative perceptions on the part of customers, counterparties, shareholders, investors, debt-holders, market analysts, other relevant parties, or regulators that can adversely affect a the Group's ability to maintain existing or establish new business relationships. [Deloitte]
Risk	The possibility that events will occur and affect the achievement of strategy and business objectives. This includes both negative effects (such as a reduction in revenue targets or damage to reputation) as well as positive impacts (that is, opportunities – such as an emerging market for new products or cost savings initiatives). [COSO 2017]
Risk Appetite	The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value. [COSO 2017]
Risk Capacity	The maximum amount of risk that an entity is able to absorb in the pursuit of strategy and business objectives. [COSO 2017]
Risk Profile	A composite view of the risk assumed at a particular level of the entity, or aspect of the business that positions management to consider the types, severity and interdependencies of risks and how they may affect performance relative to the strategy and business objectives. [COSO 2017]
Securities Settlement System	An entity that enables securities to be transferred and settled by book entry according to a set of predetermined multilateral rules. Such systems allow transfers of securities either free of payment or against payment. [IOSCO PD377]
Settlement Risk	The general term used to designate the risk that settlement in a funds or securities transfer system will not take place as expected. This risk may comprise both credit and liquidity risk. [IOSCO PD377]
Social and Relationship Capital	Networks together with shared norms, values and understandings that facilitate cooperation within or among groups. [COSO 2017]
Social Risks	Human capital, product liability, stakeholder opposition, and social opportunities. Human rights, labor standards in the supply chain, any exposure to illegal child labor and more routine issues such as adherence to workplace health and safety. A social score also rises if a company is well integrated with its local community and therefore has a *social license* to operate with consent. [COSO 2017]
Stakeholders	Parties that have a genuine or vested interest in the entity. [COSO 2017]

Strategic Risk	Strategic risks are risks that can impact business strategy execution, including affecting the Group's financial statements. Such risks may include the risk of not capturing potential gains – such as the tension between the decision to invest in product or software development and innovation versus the decision not to make this investment, which may impact the Group's bottom-line, effectiveness, and/or efficiency. [WBCSD]
Strategy	The organization's plan to achieve its mission and vision and apply its core values. [COSO 2017]
Stress Testing	The estimation of credit and liquidity exposures that would result from the realization of extreme price changes. [IOSCO PD377]
Sustainability	A business approach that creates long-term shareholder value by embracing opportunities and managing risks deriving from economic, environmental, and social developments. [COSO 2017]
Sustainability Risk	Sustainability risk is an uncertain social or environmental event or condition that, if it occurs, can cause a significant negative impact on the Group. It includes the opportunities that may be available to the Group because of changing social or environmental factors. Many sustainability risks can also be considered emerging risks, due to such risks not as prevalent or well-understood globally and regionally 20 years ago, such as consumer empowerment, climate change, and resource constraints. [WBCSD]
Systemic Risk	(1) The scenario that a disruption at a firm, in a market segment, or to a settlement system could cause a domino effect throughout the financial markets toppling one financial institution after another (e.g., the risk that the inability of one or more participants to perform as expected will cause other participants to be unable to meet their obligations when due.) [IOSCO PD377] (2) A *crisis of confidence* among investors creating illiquid conditions in the marketplace. [IOSCO PD78]
Technology Risk	The business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise. [COBIT]
Tolerance	The boundaries of acceptable variation in performance related to achieving business objectives. [COSO 2017]
Trade Repository	An entity that maintains a centralized electronic record (database) of transaction data. [IOSCO PD377]
Value Date	The value date is the day on which the payment, transfer instruction, or other obligation is due and the associated funds and securities are typically available to the receiving participant. [IOSCO PD377]

SECTION 1. STRATEGY & OBJECTIVE-SETTING

Enterprise risk management is no longer focused principally on preventing the erosion of value and minimizing risk to an acceptable level. Rather, it is viewed as integral to strategy-setting and the identification of opportunities to create and maintain value. Instead of simply focusing on reducing risk to a target state, ERM shall become a dynamic and integral part of the managing an entity throughout the value chain.

In formulating a business or operational strategy, the Group shall decide explicitly to accept some level of risk to achieve its objectives, known as *optimization*, *i.e.*, maintaining risk that is deemed acceptable within the risk appetite, which is goal of risk management. ERM shall allow the Group to improve the ability to identify risks and establish appropriate responses, reducing surprises and related costs or losses, while profiting from advantageous developments.[5] Risk and opportunity are central to business and investment strategies. Many successful businesses and investments are the result of risk-taking, and the Group is no exception.

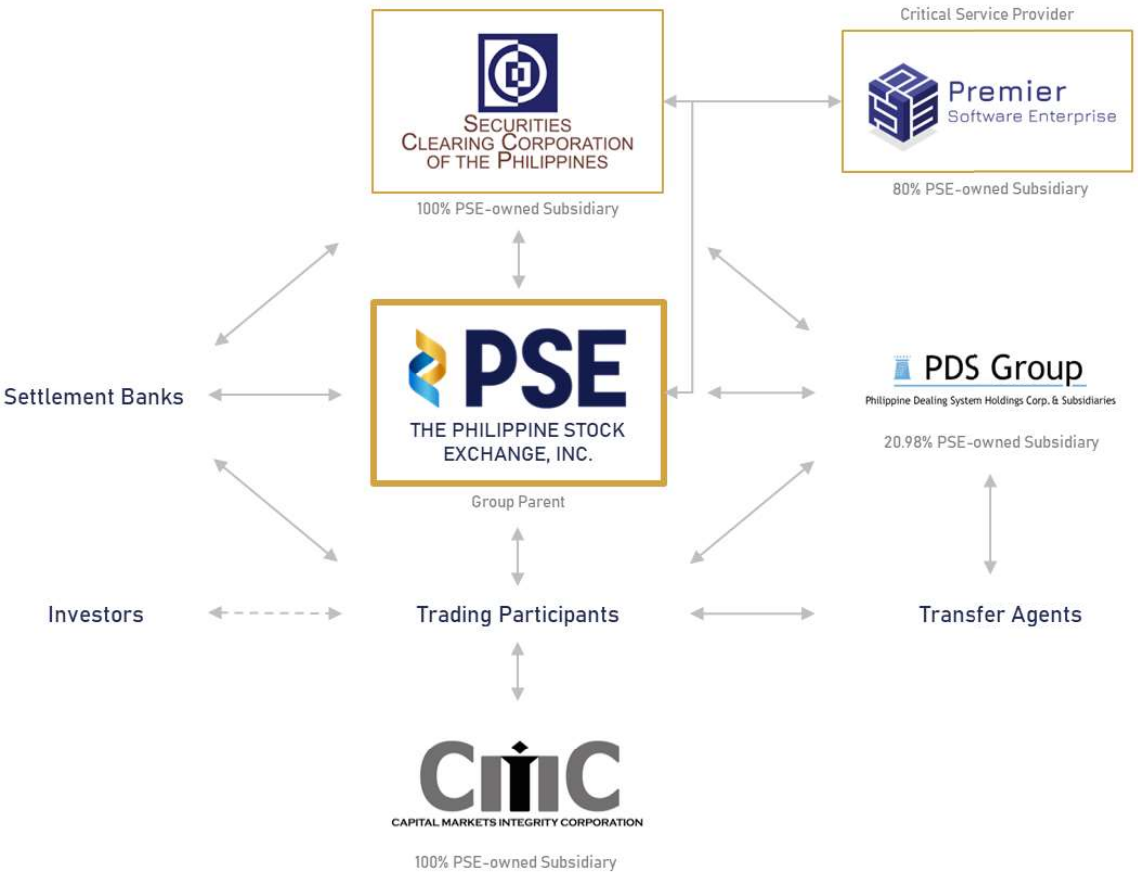
With the integration of ERM into the strategy-setting process, the setting of business objectives, and the managing of risks in the execution of the functions of the Group, risk is no longer positioned as an additional or separate activity. When Management develops a strategy and works through alternatives with the Board, decisions are made based on the trade-offs inherent in the strategy. Each alternative strategy has its own risk profile—these are the implications arising from the strategy. The Board of Directors and Management shall determine if the strategy works in tandem with the Group's risk appetite, and how it will help drive the Group to set objectives and ultimately allocate resources efficiently.[6]

Every chosen strategy must support the Group's vision and mission. A misaligned strategy increases the possibility that the Group may not realize its vision and mission, or may compromise its values, even if a strategy is successfully carried out. In this context, enterprise risk management highlights the risk of strategies of the Group not aligning with its vision and mission.

[5] COSO 2017 *Benefits of ERM Integration.*
[6] COSO 2017 *Role of Risk in Strategy Selection.*

1.1. BUSINESS ENVIRONMENT

Figure 2. Business Environment



1.1.1. The Philippine Stock Exchange, Inc. (Group Parent)

The Philippine Stock Exchange, Inc. was formed from the country's two former stock exchanges, the Manila Stock Exchange ("MSE"), established on August 8, 1927, and the Makati Stock Exchange ("MkSE"), which was established on May 27, 1963. Although both the MSE and the MkSE traded the same stocks of the same companies, the bourses were separate stock exchanges for nearly 30 years until December 23, 1992, when both exchanges were unified to become the present-day Philippine Stock Exchange.

Vision

A premier exchange with world-class standards for trading securities and raising capital that serves as a strong engine for a robust economy.

Mission

- Offer products and services responsive to the needs of investors and other stakeholders.
- Develop a highly motivated and professional workforce, committed to serve and excel.
- Be a preferred venue for raising capital.
- Operate efficiently to optimize shareholder value.
- Practice and promote good governance within the Exchange and among listed companies and trading participants.
- Adopt world-class systems and global best practices for an efficient, fair, and orderly market.
- Provide a facility for fair, accurate, complete, and timely information about listed companies, while extending market education and awareness programs to investors.

1.1.2. Securities Clearing Corporation of the Philippines ("SCCP")

SCCP is a wholly-owned subsidiary of PSE and is under the regulatory supervision of the Securities and Exchange Commission ("SEC"). It was incorporated in 1996 to operate as a central securities clearing institution in the Philippines and thereby manage and support the clearance of trades in securities listed and executed on the PSE or other official securities market in the Philippines. It acts as a Central Counterparty to trades executed at the PSE. SCCP started its commercial operations on January 3, 2000 and was granted its permanent license to operate on January 17, 2002. SCCP is authorized by the SEC to impose fines and penalties and other sanctions as approved by the SCCP Board of Directors to ensure compliance of its Clearing Members.

1.1.3. Premier Software Enterprise, Inc. ("PSEI")

Premier is 80% owned by PSE and was incorporated in 2019 as a separate IT subsidiary to enable the Exchange to meet the growing demand for technology services related to its various initiatives. Premier is tasked to build innovative trading solutions, further automate critical Exchange processes, and explore new technologies such as cloud services, among others. As an institution heavily reliant on technology and focused on maintaining reliable and resilient operational systems, expanding the IT capabilities of PSE through Premier will help improve the Exchange's products and services.

1.1.4. Capital Markets Integrity Corporation ("CMIC")

CMIC is a wholly-owned subsidiary of PSE and was established for the primary purpose of reinforcing the confidence of the investing public in capital market institutions and promoting a more active and vibrant market participation. Accordingly, CMIC acts as the independent audit, surveillance, and compliance arm of the Exchange. As a self-regulatory organization, CMIC's primary mandate is to maintain the integrity of the market and minimize the risk of the investing public by ensuring that the TPs adhere to all pertinent rules, regulations, and code of conduct of CMIC and the Exchange, as well as all related legislative and regulatory requirements. Tasked with regulating and monitoring the activities of market participants, CMIC enforces rules, guidelines, and provisions of the Securities Regulation Code, or the SRC, and other securities laws, applicable to the operations and dealings of the TPs of – including, in particular cases, Issuers whose securities are listed in – the Exchange. Verily, under the CMIC Rules, which took effect in March 2012, CMIC, among other matters, enforces compliance by TPs – and, in the proper cases, by Issuers – with the securities laws.

SECTION 2. RISK GOVERNANCE, MANAGEMENT & CULTURE

2.1. GOVERNANCE STRUCTURES & RESPONSIBILITIES[7]

Managing risk is part of governance and leadership, and is fundamental to how the Group is managed at all levels.[8] Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for enterprise risk management.[9] Governance provides the processes through which the Group sets its objectives, determines the means for achieving those objectives, and monitors performance against those objectives. Good governance provides the proper incentives for a financial market infrastructure's Board and Management to pursue objectives that are in the interest of the Group's stakeholders and that support relevant public interest considerations.[10]

The Group aims to maintain governance arrangements that are clear and transparent, promote the safety and efficiency of the financial market infrastructure, and support the stability of the broader financial system and other relevant public interest considerations, and the objectives of relevant stakeholders. Governance arrangements ensure that the risk management and internal control functions have sufficient authority, independence, resources, and access to the Board.[11]

2.1.1. Board of Directors[12]

The Board and Senior Management are ultimately responsible for managing the risks of the Group. The Board shall determine an appropriate level of aggregate risk tolerance and capacity for the Group. The Board and Senior Management shall establish policies, procedures, and controls that are consistent with the Group's risk tolerance and capacity. Policies, procedures, and controls serve as the basis for identifying, measuring, monitoring, and managing the Group's risks and cover routine and non-routine events, including the potential inability of a participant, or the Group itself, to meet obligations.[13]

[7] Refer to the *Manual on Corporate Governance* for other governance roles and responsibilities.
[8] ISO 31000 *Risk Management*.
[9] COSO 2017 *Governance and Culture.*
[10] IOSCO PD377 *Principle 2: Governance.*
[11] Ibid.
[12] Responsibilities of the Board mentioned in this manual may be delegated to the Risk Management Committee. However, accountability for the effective design and implementation of the ERM framework still resides with the Board.
[13] IOSCO PD377 *Principle 3: Framework for the Comprehensive Management of Risks.*

The Board shall regularly monitor the Group's risk profile to ensure that it is consistent with the Group's business strategy and risk tolerance policy. In addition, the Board shall ensure that the Group has an effective system of controls and oversight, including adequate governance and project management processes, over the models used to aggregate and manage the risks of the Group. Board approval shall be required for material decisions that would have a significant impact on the risk profile of the Group, such as the limits for total credit exposure and large individual credit exposures. Other material decisions that may require Board approval include the introduction of new products, use of new crisis management frameworks, adoption of processes and templates for reporting significant risk exposures, and adoption of processes for considering adherence to relevant market protocols.[14]

2.1.2. Nominations & Elections Committee

The Board shall be composed of suitable members with an appropriate mix of skills (including strategic and relevant technical skills), experience, and knowledge of the entity (including an understanding of the Group's interconnectedness with other parts of the financial system). Board members shall also have a clear understanding of their roles in corporate governance, be able to devote sufficient time to their roles, ensure that their skills remain up-to-date, and have appropriate incentives to fulfil their roles. Board members shall exercise objective and independent judgment. Independence from the views of management typically requires the inclusion of non-executive Board members, including independent Board members, as appropriate.[15]

The Nominations and Elections Committee ("NOMELEC") is an independent committee whose creation has been mandated by the Exchange's Manual on Corporate Governance and the Securities Regulation Code ("SRC"). The NOMELEC shall formulate, screen, evaluate, and study qualifications of the Board of Directors, as well as those recommended to other positions requiring appointment by the Board. It is likewise tasked with completing the list of directors for nominations in accordance with the SRC as well as finalizing such rules and regulations it may formulate within its jurisdiction for approval by the Board.

[14] IOSCO, *supra* note 10.
[15] Ibid.

2.1.3. Investments Committee

The Investment Committee shall oversee the management of the investment portfolio of the Group and to formulate investment policies, guidelines and strategies, guided by the general objective of preserving the investible funds of the Group and maximizing returns while eliminating undue exposure to risks. The Committee shall set the investment risk limits and impose such other conditions as may be necessary to protect the interests of the Group.

2.1.4. Corporate Governance Committee

The PSE Board shall be fully committed to aligning the Group's corporate governance ("CG") practices to internationally accepted standards. As such, it has designated the CG Committee to assist the Board of Directors on issues directly connected with:

- The Group's internal processes, work procedures, and performance;
- The performance of the President and his Management team;
- Compensation, benefits and incentives;
- Succession planning;
- The overall corporate governance of the Group; and
- Market governance.

2.1.5. Risk Management Committee

The Risk Management Committee ("RMC") shall provide oversight and guidance on the management of risks faced by the Group, oversee the risk management framework of the Group; and review risk management policies and processes for the reporting of risks. The Committee shall also review different components of the capital markets (*i.e.*, products, participants, activities). In view of IOSCO Principle 7 which requires ongoing assessment of the regulatory perimeter, review shall include regulated and unregulated activities. To achieve this, the Committee shall use inputs generated by various operating divisions and combines it with market intelligence, data, and research analysis performed by a centralized risk, research, and strategy function.

The Committee shall be chaired by a sufficiently knowledgeable individual who is independent of the Group's executive management and shall be composed of a majority of members who are non-executive members. The Committee shall have a clear and public mandate and operating procedures

and, where appropriate, have access to external expert advice.[16] In addition, the Committee shall be responsible and accountable for providing effective oversight of the Group's risk profile. In particular, the RMC shall ensure that the Group's Senior Management is effectively governing and managing the Group's risk environment.

2.1.6. Compliance Office

The Group shall have comprehensive internal processes to help the Board and Senior Management monitor and assess the adequacy and effectiveness of risk management policies, procedures, systems, and controls. While business line management shall serve as the Group's first line of defense ("LOD") and risk management and compliance functions as the second, the adequacy of and adherence to control mechanisms shall be assessed regularly through independent compliance programs/testing and independent audits.

2.1.7. Internal Audit

As the third LOD, a robust internal audit function shall provide an independent assessment of the effectiveness of the Group's risk management and control processes. An emphasis on the adequacy of controls by Senior Management and the Board, as well as internal audit shall help counterbalance a business management culture that may favor business interests over establishing and adhering to appropriate controls. In addition, proactive engagement of audit and internal control functions when changes are under consideration shall be beneficial. Specifically, the involvement of the internal audit function in pre-implementation reviews often reduces the need to expend additional resources to retrofit processes and systems with critical controls that had been overlooked during initial design phases and construction efforts.[17]

[16] IOSCO, *supra* note 10.
[17] IOSCO, *supra* note 13.

2.2. SUBSIDIARY GOVERNANCE

For effective oversight of the subsidiaries, especially for operating subsidiaries which are of strategic importance to the Parent or contributes significantly[18] to the Parent's operations, the Board of the Parent shall devote sufficient time to oversee the business and risks of such subsidiaries, especially on critical areas which shall engage the attention of the Parent. The Parent's Board shall control the strategic direction of the Group as a whole.

However, the subsidiary Boards shall also be doing much more than merely reflecting management of the subsidiary. Careful thought on the design of the subsidiary Boards shall be required, which shall help the subsidiary Boards add considerable value to the Group, pay closer attention to the compliance processes within the subsidiary, and ensure there are no gaps in oversight.

For achieving the objectives of independence and coordination, subsidiaries shall also select Directors from outside the management of the subsidiaries, either from unrelated businesses or from the Parent's Board. Such setup shall ensure consistency in strategic direction and shall also provide a useful connection between the Parent's Board and subsidiary Boards.[19]

Approval levels and decision-making shall follow Group-level policies and guidelines while approval of transactions shall be required at the Parent Board level if such transactions are significant enough. Significant transactions or arrangements shall mean any individual transaction or arrangement that exceeds or is likely to exceed 10% of the total revenues or total expenses or total assets or total liabilities, as the case may be, of the material subsidiary for the immediately preceding accounting year.

Further, corporate governance-related policies and procedures shall developed centrally[20] by the Group and shall be required to be implemented in all parts of the Group without regard to the legal subsidiary structure.[21]

It shall be equally important for the Board to ensure that the information flow among the subsidiaries and the Parent is timely and comprehensive in the identified critical areas. This oversight shall be achieved through internal management interactions and reporting requirements, through oversight of the

[18] Refer to **Annex F** for the tiering of subsidiaries according to significance.
[19] Deloitte *Governance of Subsidiaries.*
[20] Larger groups require more uniform implementation of key policies, such as whistleblower policy, across the entire group regardless of the size and location of subsidiaries.
[21] Deloitte, *supra* note 19.

Parent's Board, or a combination of both. The risks of downstream governance failures can have devastating impacts on the Group as a whole.[22] The Group, TPs, critical service providers ("CSPs"), and other related entities shall share among each other relevant information to manage and contain risks vis-à-vis the FMI.

2.3. GOVERNANCE OF CRITICAL SERVICE PROVIDERS

The operational reliability of the Group depends on the continuous and adequate functioning of third-party service providers that are critical to the Group's operations – PSEI for the PSE Group. The continuous, secure, and efficient delivery of essential services by third-party service providers may also negatively impact other FMIs.[23]

2.3.1. Governance

The identification and management of risks shall be overseen by the CSPs' Board of Directors and assessed by an independent, internal audit function that can communicate clearly its assessments to relevant Board members. The Board is expected to ensure an independent and professional internal audit function. The internal audit function shall be reviewed to ensure it adheres to the principles of a professional organization that governs audit practice and behavior (such as the Institute of Internal Auditors, "IIA") and is able to independently assess inherent risks as well as the design and effectiveness of risk management processes and internal controls. The internal audit function shall also ensure that its assessments are communicated clearly to relevant Board members.[24]

2.3.2. Risk Management

CSPs shall have effective processes and systems for identifying and documenting risks, implementing controls to manage risks, and making decisions to accept certain risks. CSPs also face risks related to information security, reliability and resilience, and technology planning, as well as legal and regulatory requirements pertaining to its corporate organization and conduct, relationships with customers, strategic decisions that affect its ability to operate as a going concern, and dependencies on other third parties. CSPs shall reassess their risks, as well as the adequacy of their risk management frameworks in addressing the identified and emerging risks, on an ongoing basis.[25]

[22] Ibid., 25.
[23] IOSCO PD432 *Assessment Methodology for the Oversight Expectations Applicable to Critical Service Providers.*
[24] IOSCO PD432 *OE1. Risk Identification and Management.*
[25] Ibid.

CSPs shall have effective technology planning that minimizes overall operational risk and enhances operational performance. Planning shall entail a comprehensive information technology strategy that considers the entire lifecycle for the use of technologies and a process for selecting standards when deploying and managing services. Proposed changes to CSPs' technologies shall entail a thorough and comprehensive consultation with the Group and, where relevant, TPs. CSPs shall regularly review their technology plans, including assessments of their technologies and the processes used for implementing change. CSPs shall place robust methods to plan for the entire lifecycle of the use of technologies and the selection of technological standards.[26]

CSPs shall implement a robust information security framework that appropriately manages information security risks. The framework shall include sound policies and procedures to protect information from unauthorized disclosure, ensure data integrity, and guarantee the availability of its services. In addition, CSPs shall maintain policies and procedures for monitoring their compliance with its information security framework. The framework shall also include capacity planning policies and change management practices.[27]

2.3.3. Incident Management

CSPs shall provide reliable and resilient operations to users, whether these operations are provided to the Group directly or to the Group and TPs. CSPs shall have robust operations that meet or exceed the needs of the Group. Any operational incident shall be recorded and reported to the Group. CSPs shall analyze incidents promptly to prevent recurrences that could have greater implications.

In addition, CSPs shall have robust business continuity and disaster recovery objectives and plans. These plans shall include routine business continuity testing and a review of these test results to assess the risk of a major operational disruption. Plans shall therefore support the timely resumption of critical services in the event of an outage so that the service provided fulfills the terms of the CSPs' agreements with the Group.[28]

[26] IOSCO PD432 *OE4. Technology Planning.*
[27] IOSCO PD432 *OE2. Information Security.*
[28] IOSCO PD432 *OE3. Reliability and Resilience.*

2.3.4. Communication & Reporting

CSPs shall have effective customer communication procedures and processes. In particular, CSPs shall provide the Group and, where appropriate, TPs, with sufficient information so that users clearly understand their roles and responsibilities, enabling them to manage adequately their risks related to their use of the services provided. Useful information for users typically includes, but is not limited to, information concerning the CSPs' management processes, controls, and independent reviews of the effectiveness of these processes and controls. As a part of its communication procedures and processes, CSPs shall establish mechanisms to consult with users and the broader market on any technical changes to its operations that may affect its risk profile, including incidences of absent or non-performing risk controls of services. In addition, CSPs shall have a crisis communication plan to handle operational disruptions to its services.[29]

2.4. REGULATORY PERIMETER GOVERNANCE: TP SUPERVISION

Effective reporting procedures can only be maintained if the Group has in place a good information system which will permit accurate and detailed information to be retrieved in a timely and reliable manner. The Group's ability to gather and accurately interpret necessary financial and operational information relating to the control environment is critical to effective supervision. TPs shall provide the Group with relevant information about the use of controls in each firm and about significant control failures under routine and in emergency situations. The Group shall have mechanisms to share information about controls with each other during these situations. The Group's information needs relating to controls will often be sharply focused and potentially very detailed in any emergency situation.[30]

The responsibilities of the Group in jurisdictional arrangements to review the regulatory perimeter shall allow for the identification of risks posed by unregulated products, markets, market participants, and activities. Arrangements shall consider the potential for regulatory arbitrage, which might emerge outside the Group's mandate but may affect the discharge of its statutory functions (even where the Group does not have the explicit power to intervene). In such instances, the Group shall raise awareness of issues or to pass them on to other relevant authorities within its jurisdiction to act. This action may include seeking to introduce requirements under its rule-making powers or seeking changes in legislation. These arrangements shall:

[29] IOSCO PD432 *OE5. Communication with Users.*
[30] IOSCO PD78 *Section IV. Reporting.*

- Involve other securities regulators systematically identifying, prioritizing, and determining the scale and scope of emerging risks from different entities, activities, markets, and products in financial markets that could serve as the basis for deciding whether and what type of regulatory action or intervention is warranted;
- Build on existing risk identification frameworks by requiring securities regulators to proactively go beyond existing regulatory boundaries to identify potential risks; and
- Recognize that different approaches may be required to discern and assess different types of risks; just as having a single perspective may not prove effective, having only one risk approach similarly may not suffice. For example, a different approach may be warranted for known risks that are being re-evaluated, as opposed to emerging risks being considered for the first time, particularly if they are emerging outside of the regulatory perimeter.[31]

2.5. RISK CULTURE

A risk-aware culture[32] promotes open discussions of risk, and acceptable levels of risk are understood and maintained. A risk-aware culture begins at the top, with Board members and business executives who set direction, communicate risk-aware decision-making, and reward effective risk management behaviors. Risk awareness also implies that all levels within the Group understand how and why the Group responds to key risk events. Risk culture includes:

- Behavior towards taking risk[33]
- Behavior towards policy[34]
- Behavior towards negative outcomes[35]

The Group shall build an organizational culture that supports and serves as a foundation to processes in relation to systemic risk and reviewing of the regulatory perimeter, with the view of achieving its strategic objectives. The Group shall ensure awareness of their systemic risk and regulatory perimeter review arrangements and commitment to the effective and meaningful operation of such

[31] IOSCO PD443 *Systems/Processes: Regulatory Perimeter Arrangements.*
[32] Refer to **Annex K** for more details on risk culture.
[33] What are the norms and attitudes towards risk-taking, identification of risk, and analysis of risk?
[34] Is policy something that exists but is not followed? Do policies drive behavior? Are policies easy to read, understand, and follow?
[35] How does the Group deal with negative outcomes, policy exceptions, loss events, cyber incidents, missed opportunities, and incident investigations? Will it learn from them and try to adjust, or will blame be assigned without treating the root cause?

arrangements (including promotion of professional skepticism) as key elements of the organizational culture.[36]

The relationship between culture and business influences how strategies are chosen and executed. More importantly, culture provides the context for the identification and assessment of risks and the allocation of resources in responding to those risks.

2.6. LINES OF DEFENSE[37]

The Group does not operate in a risk-free environment, and the implementation of ERM does not create such an environment. Rather, the Group operates in environments filled with uncertainty, requiring proactive action to address risks in order to survive and prosper. Effective ERM involves the strategic implementation of three lines of defense. At each line of defense there are risk governance guidance (i.e., Senior Management, RMC, Board) to support the ERM framework.

2.6.1. First Line of Defense

The *first line of defense* is the front-line employees who must understand their roles and responsibilities with regard to processing transactions and who must follow a systematic risk process and apply internal controls and other risk responses to treat the risks associated with those transactions. Line management shall be responsible to identify and assess risks and to ensure that the control activities and other responses that treat risk are enforced and monitored for compliance.

The information that line management shall report to Risk Management may include, but is not limited to:

- Risk footprint, heat map (highly rated residual risks)
- Key risk issues, planned mitigation actions, and responsible action owners
- Status of existing mitigation actions
- Key risk indicators (red or amber)
- Control effectiveness indicators (red or amber)
- Incidents and breakages (including historical/trend analysis/statistics, status of mitigation actions and lessons learned)
- Outstanding deficiencies or internal/external audit items that are past their action due date

[36] IOSCO, *supra* note 31.
[37] Refer to **Annex D** for more detailed discussion on the lines of defense.

However, the implementation of the tools and techniques above shall be commensurate with the maturity of line management's risk culture and practice. Line management shall involve the Group's ERM function in key risk meetings in order to timely assist in the management of key risks vis-à-vis the achievement of enterprise strategy and business objectives. Alternatively, the risk report and minutes of line management's key risk meetings shall be forwarded timely to the ERM function for review. This information[38] shall then be collated with other risk reports and assessed and reported, based on criticality, both independently and directly, to either Senior Management and/or RMC, who are charged with the role of representing the Group's stakeholders with respect to risk issues.

2.6.2. Second Line of Defense

The *second line of defense* is the Group's compliance and risk functions that provide independent oversight of the risk management activities of the first line of defense. The risk function shall have its own governance committee ("RMC") and the compliance function shall have a direct reporting line to the Board. The responsibilities of second-line functions typically include participating in the business units' risk meetings, reviewing risk reports, and validating compliance with the risk management framework requirements, with the objective of ensuring that risks are actively and appropriately managed.

Governance & Management of the Risk Management Function[39]

The Group's risk management personnel shall have sufficient independence, authority, resources, and access to the Board to ensure that the operations of the Group are consistent with the ERM framework set by the Board. The reporting lines for risk management shall be clear and separate from those for other operations of the FMI and there shall be a direct reporting line to a non-executive director on the Board via a Chief Risk Officer (or equivalent). To help the Board discharge its risk-related

[38] The second (risk and compliance) and third (audit) lines of defense often request the same information as the first-line management and governance committees. In practice, often this independently assessed risk information conveys a mixed message with the result that there is an arc of miscommunication, *i.e.*, what is reported does not always align with the risk reality as perceived by front-line management. This difference in perspective is what adds value to the enterprise as a whole and to the ERM framework in particular. It is for the senior enterprise risk governance committee to evaluate the reports from these multiple sources and determine (or advise the main Board on) the direction the enterprise should take.

[39] Refer to **Annex A** for the *Risk Management Committee Charter* and **Annex B** for the responsibilities of the Chief Risk Officer.

responsibilities, the RMC shall be responsible for advising the Board on the Group's overall current and future risk tolerance and strategy. The RMC shall have a clear and public mandate and operating procedures and, where appropriate, have access to external expert advice.[40]

2.6.3. Third Line of Defense

The *third line of defense* is that of internal and external auditors who report independently to the Audit Committee. The results of independent reviews shall be effectively communicated to Senior Management and, more importantly, to the Board in cases in which these groups ensure that appropriate action is taken to maintain and enhance the ERM framework.

[40] IOSCO, *supra* note 10.

SECTION 3. FRAMEWORK EXECUTION

3.1. RISK IDENTIFICATION

The first step in setting a risk management and control strategy is a formal analysis of Group's business activities and the risks of these activities to the Group, ultimately in terms of the risk to capital.[41] In addition, the Group shall take a broad, integrated, and comprehensive perspective of its risks and identify the risks the Group directly bears from or poses to TPs, settlement banks, liquidity providers, service providers, and any other entities that could materially be affected or affect the Group's ability to provide services.

Venues for risk identification may include, but are not limited to:

- Risk Roundtables
  - Strategic Planning Sessions
  - Board/Committee/Functional/Business Meetings
- Research & Industry Experts
  - Internal Periodic Reports
  - Corporate Governance Committee
  - Risk Management Committee
  - IOSCO Risk Dashboard
  - IOSCO Dialogues thru Committee on Emerging Risks[42]
  - IOSCO Securities Markets Risk Outlook Publication
  - Publications on Investor Behavior and Market Structures
- Other Risk Management Venues
  - Incident/Problem Management
  - Contract/Vendor Management
  - Performance Management, Key Performance Indicators
  - Risk and Control Self-assessments, Key Risk Indicators
  - Surveys on Risk Culture & Awareness
  - Data Analytics
  - Compliance Programs
  - Internal Audits
  - External Audits

Upon identification, material risks which may significantly impact the achievement of strategy and business objectives shall be communicated to the risk owner in writing for proper risk response. The risk owner shall be responsible for the maintenance and timely update of material risks in the risk register.

[41] IOSCO PD78 *Section III. Firm and Supervisory Considerations.*

[42] The CER meets three or four times annually. A key target of the CER meetings is to foster an active and open dialogue on risk among CER members who represent a large number of jurisdictions.

3.2. RISK OWNERSHIP

Although Management collectively owns the entity risks, the risk owner shall be the point person with accountability for ensuring specific risks are properly managed. Such person must be closely related to processes and operations where the risks have been identified and shall be someone who would *feel the pain* when the risks materialize. However, such risk owner must be also positioned highly enough[43] in the Group to take consequent action, charged with the accountability and authority to manage the risks identified, preferably who belongs to senior leadership. [44] The risk treatment plan shall be the primary venue for the appointment of risk owners.

3.3. RISK ASSESSMENT

Assessment of the effectiveness and risk of established strategies, policies, and procedures shall be performed regularly. The evaluation shall consider the results of established policies, changes in business activities, and changes in markets. Material changes to methodologies, models, and assumptions of risk management and control policies shall be reviewed by the Board. Policies and procedures shall require that the risk management and control functions be involved in the review of new business products and activities. *Risks* shall be assessed in terms of significance, likelihood, and potential impact on the achievement of strategic plans and business objectives. *Significance* shall be according to the expert judgment of the Board and Senior Management. *Likelihood* shall be the probability of the risk materializing, which shall be assessed vis-à-vis the extent to which the risk materializing would affect the Group's achievement of its strategic goals and business objectives (*impact*).

Figure 4. Risk Rating Matrix

		Impact		
		Minor	Moderate	Major
Likelihood	Almost Certain	Moderate	High	High
	Possible	Low	Moderate	High
	Rare	Low	Low	Moderate

[43] Without resources, the task would be impossible.
[44] Refer to **Annexes C, D,** and **E** for the risk ownership structure across the Group.

Further, risk assessment shall be performed at the following levels[45]:

- *Inherent risk* is the risk to the Group in the absence of any actions Management might take to alter either the risk's likelihood or impact. It is the risk without the application of any control mechanisms.
- *Residual risk* is the risk remaining after Management's response to the risk. It is the risk after the application of control mechanisms.

3.4. CONTROL ENVIRONMENT

The Group shall concern itself with understanding the control environment of each member of the Group, and satisfying itself as to the adequacy of controls established by Management. Supervisors shall be responsible for regulating the activities of securities firms in order to protect investors in the securities markets and ensure the integrity of those markets. To this end, the Group must be proactive, rather than reactive, in devising high quality supervision of the dynamic securities industry.[46]

The control culture shall be expanded to all staff levels, with a view to promoting a widely shared control culture within the Group, since the control environment sets the tone of an organization, influencing the control consciousness of its people. The Group's control culture shall be the foundation for all other components of internal control, providing discipline and structure.[47] To influence risk culture, entity-level controls shall be effective in managing key risks to strategies and business objectives. Entity-level controls[48] are internal controls which help to ensure that Management directives pertaining to the entire Group are carried out effectively. Entity-level controls have a pervasive influence throughout the Group. If such controls are weak, inadequate, or non-existent, key risks exposures may not be contained/controlled.[49]

The control environment's effectiveness is influenced by several variables[50], including:

- Board/Management's Attitudes, Beliefs, and Practices
- Organizational Structure and Accountability
- Nature and Scope of the Governing Bodies and Management Committees
- Degree of External Oversight

[45] COSO 2017 *Enterprise Risk Management Framework: Integrating with Strategy and Performance.*
[46] IOSCO, *supra* note 41.
[47] IOSCO PD78 *Section IV. Elements of a Risk Management and Control System.*
[48] Refer to **Annex Q** for examples of entity-level controls.
[49] COSO, *supra* note 45.
[50] IOSCO, *supra* note 47.

3.5. RISK TOLERANCE, APPETITE & PRIORITIZATION[51]

Tolerance is the amount of risk that is acceptable for a given level of performance. The determination of those boundaries enables the Group to better assess whether changing levels of performance remain within the limits of acceptable variation. No longer are risk and performance considered static and separate, but rather, constantly changing and influencing one another. Risk tolerance shall be defined at the Board/Senior Management level and shall be reflected in policies set by the executives; at lower (tactical) levels of the Exchange/Group, exceptions can be tolerated (or managed according to varying defined thresholds) as long as the overall exposure does not exceed the risk appetite. Any business initiative includes a risk component, therefore Management shall have the discretion to pursue new opportunities of risk. The better risk management the Group has in place, the more risk can be taken in pursuit of return.

Risk appetite is the amount of risk willing to be accepted in the pursuit of strategy and business objectives. Effective risk management begins at the highest levels of the Group which may be supported with well-formed and articulated risk appetite statements. The statements, when clearly understood, communicated and practiced, serve as the guide to the behaviors, decisions, limits and policies that provide the boundaries under which risk management practices operate within the Group. Risks shall then be prioritized[52] by severity in the context of risk appetite.

3.6. RISK TREATMENT

After consideration of the control environment, the Group shall take a portfolio view of the amount of residual risk and select appropriate risk responses. Risk responses shall be required for residual risks rated as high and moderate, choosing at least one (1) among the following risk treatment plans:

- **Reduce**: Action taken to lessen the probability and/or impact of a risk
- **Transfer**: Action to transfer or redistribute a part of a risk to a third party
- **Avoid**: Action taken to cease or not start activities leading to a risk
- **Accept**: Action taken based on an informed decision not to reduce, transfer, or avoid the probability and/or impact of a risk

[51] COSO, *supra* note 45.
[52] Refer to **Annex L** for guidance on prioritization.

Appropriate mitigation actions[53] from the risk owner/s may include:

- **Policy Action**
  (including circulars, statements of regulatory expectations, or changes in rules and regulations)
- **Communication & Coordination**
  (internally and/or externally)
- **Changes to the Strategic Prioritization of the Group**
  (including resource allocation and supervisory or enforcement prioritization)

Implementation procedures shall be performed to effectively carry out Management's wishes regarding the controls that need to be established in the Group. Without effective implementation procedures, the best system of controls would be nothing more than a facade. High-profile losses may occur despite the existence of documentations of control systems if controls would not be properly implemented by the Group.[54]

3.7. REVIEW & MONITORING

By reviewing the Group's performance, the Group shall be able to consider how well the enterprise risk management components have been functioning over time and in light of substantial changes, and what revisions are needed. Consequently, a risk management and control reporting and review process shall include a review mechanism for reporting compliance with established policies and procedures and addressing exceptions.[55]

3.7.1. Strategic Alignment

The alignment among the strategic plan, business objectives, vision, mission, culture/core values, and the ERM framework shall be reviewed by Senior Management at least annually and when significant changes have occurred which may result in any misalignment that may hinder the Group from achieving its strategic and business objectives.

3.7.2. Enterprise Risk Management Framework

As the Group's risk management culture and practice achieves a higher level of maturity and when there are significant changes in the business

[53] IOSCO PD443 *Chapter 3: Risk Identification Methods used by Securities Regulators.*
[54] IOSCO, *supra* note 47.
[55] IOSCO, *supra* note 41.

environment which may merit prompt review and revision of the ERM framework by Senior Management and the Board, more advanced risk management tools and techniques may be introduced, commensurate with the requirements of the Group vis-à-vis strategic requirements and business objectives.

3.7.3. Risk vs. Performance

CMIC shall monitor the financial condition of TPs while the Exchange shall monitor the same for CSPs, via reporting requirements and on-site examinations, which may performed in coordination with other regulatory authorities. Such activities are designed to allow the CMIC/PSE, as a regulator, to identify TPs and CSPs experiencing financial or operational difficulties at an early stage. This provides the opportunity to work with the TP or CSP to implement steps to increase its solvency or, if necessary, begin the process of an orderly liquidation. TPs and CSPs shall also be required to provide the Group timely notice when their net capital level falls below early warning levels (which are set above the minimum requirements) and when they withdraw capital above certain threshold amounts. Generally, Internal Audit shall have oversight over CSPs' yearly audit by an independent auditor to verify the information in the periodic reports.[56]

3.7.4. Verification

Verification is an essential element of any risk management and control system. Without a comprehensive set of verification procedures by the Group, TPs and CSPs, the risk of a breakdown in controls somewhere in the FMI increases. Controls, once established by Management, shall be verified as operating as designed and updated in accordance with new products and industry technology. Verification procedures relating to controls shall be a function of internal and external oversight with four levels of defense[57]:

- First LOD
- Second LOD
- Third LOD
- Securities and Exchange Commission and/or External Audit

In addition, external audits by independent accountants which cover at least the internal accounting control systems shall be part of a TP's and

[56] IOSCO PD122 *Section III. Supervisory Approaches and Capital Regulation: Securities Regulation.*
[57] Refer to **Annex D** for more details on the lines of defense.

CSP's annual procedures and shall also be mandated by the Group or the Securities and Exchange Commission ("SEC").

3.7.5. Emerging Risks

The Group shall regularly review the material risks it bears from and poses to other entities (such as other FMIs, settlement banks, liquidity providers, or service providers) as a result of interdependencies and develop appropriate risk management tools to address these risks. In particular, the Group shall have effective risk management tools to manage all relevant risks, including the legal, credit, liquidity, general business, and operational risks that it bears from and poses to other entities, in order to limit the effects of disruptions from and to such entities as well as disruptions from and to the broader financial markets. These tools shall include business continuity arrangements that allow for rapid recovery and resumption of critical operations and services in the event of operational disruptions, liquidity risk management techniques, and recovery or orderly wind-down plans should the FMI become non-viable. Because of the interdependencies between and among systems, the Group shall ensure that its crisis management arrangements allow for effective coordination among the affected entities, including cases in which its own viability or the viability of an interdependent entity is in question.[58]

3.8. REPORTING

Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization. [59] Reporting is an integral part of the organization's governance and shall enhance the quality of dialogue with stakeholders and support Senior Management and oversight bodies in meeting their responsibilities. Factors to consider for reporting may include, but are not limited to[60]:

- Different stakeholders and their specific information needs and requirements
- Cost, frequency, and timeliness of reporting
- Method of reporting
- Relevance of information to the group's strategic plan, business objectives, and decision-making

[58] IOSCO, *supra* note 13.
[59] Refer to **Annexes C, D,** and **E** for the *Parent and Group Risk Ownership and Reporting Structure*.
[60] ISO 31000 *Section 7: Recording and Reporting*.

Risk reporting shall be on the potential or actual manifestations of risk impacting performance and the achievement of strategy and business objectives. Risk assessments and risk reporting are not intended to generate long lists of potential risks, but shall rather highlight how risks may impact the achievement of strategy and business objectives.

Communication of Key Risks & Control Gaps

Reporting on the adequacy of risk management and controls shall be necessary to maintain an effective and efficient control environment within the Group. The Exchange/Group, as a regulator, shall require the establishment of mechanisms to report material inadequacies or breakdowns in controls to the Group on a timely basis. Without timely reporting procedures about breakdowns in controls, the effectiveness of controls would be diminished due to the loss of essential and timely information that may be crucial to the decision making process of the Group and market participants.[61]

TPs shall be prepared to provide the Group with relevant information about the use of controls their respective jurisdictions and about control failures under routine and in emergency situations. Effective reporting procedures can only be maintained if the FMI, as a whole, has in place a good information system which will permit accurate and detailed information to be retrieved in a timely and reliable manner.

The Group shall have mechanisms to share information about controls within the FMI, as necessary. The Group's information needs relating to controls will often be sharply focused and potentially very detailed in any emergency situation. While the primary information needs in an emergency situation will be firm-specific, there may also be a need for information relating to depositories, exchanges, and clearing organizations.[62]

[61] IOSCO, *supra* note 47.
[62] Ibid.