GSIS Government Service Insurance System
Financial Center, Pasay City, Metro Manila 1308

OFFICE OF THE CORPORATE SECRETARY

EXACT COPY OF RES. NO. 26 ADOPTED BY THE GSIS BOARD OF TRUSTEES IN ITS MEETING NO. 4 HELD ON 23 FEBRUARY 2021

Approval of the Amendment of the Risk Oversight Committee Charter[1]

RESOLUTION NO. 26

WHEREAS, the Risk Oversight Committee Charter was last updated through Board Resolution No. 27 dated 27 February 2019;

WHEREAS, the Corporate Secretary proposed several amendments to the said Charter to institutionalize current practices already being performed by the concerned functional groups and offices, update existing provisions particularly on the conduct of virtual meetings, and to give certain provisions a more orderly, logical, and systematic arrangement;

WHEREAS, the Risk Oversight Committee issued Resolution No. 20013-21 dated 8 February 2021, endorsing the amendments to the Risk Oversight Committee Charter for Board approval, subject to certain amendments, which the Corporate Secretary have incorporated;

RESOLVED, to **APPROVE** and **CONFIRM** the amendments to the Risk Oversight Committee Charter, as submitted by the Corporate Secretary in her memorandum dated 15 February 2021.

[1] Classification: Internal Use

A copy of the amended Risk Oversight Committee Charter is made an integral part of this Resolution.

CERTIFIED CORRECT:

ORIGINAL SIGNED
ATTY. LUZ VICTORIA F. REYES-MORANDO
Corporate Secretary

CONFIRMED:

ORIGINAL SIGNED
LUCAS P. BERSAMIN
Chairman

ORIGINAL SIGNED
ROLANDO L. MACASAET
Vice Chairman

ORIGINAL SIGNED
WILFREDO C. MALDIA
Trustee

ORIGINAL SIGNED
JOCELYN DE GUZMAN CABREZA
Trustee

ORIGINAL SIGNED
ALAN R. LUGA
Trustee

ORIGINAL SIGNED
NINA RICCI A. YNARES-CHIONGBIAN
Trustee

ORIGINAL SIGNED
ANTHONY B. SASIN
Trustee

ORIGINAL SIGNED
KAHAR H. MACASAYON
Trustee

ORIGINAL SIGNED
CARLO ANTONIO B. ALMIRANTE
Trustee

GOVERNMENT SERVICE INSURANCE SYSTEM
BOARD OF TRUSTEES

CHARTER OF THE RISK OVERSIGHT COMMITTEE

(as amended on _____)

The Risk Oversight Committee Charter ("Charter") establishes the purpose, membership and qualifications, authority, duties and responsibilities, of the Risk Oversight Committee to serve as guide in the performance and conduct of its functions. (n)

1. GENERAL PURPOSE AND AUTHORITY

The Risk Oversight Committee (ROC) is organized to assist the GSIS Board of Trustees in carrying out its responsibilities for policy formulation and for oversight of System-wide risks, including compliance with applicable laws and regulations.

The ROC shall likewise perform oversight functions of all Information Technology (IT) and Information Security matters.

2. REPORTING

The ROC shall work under the direction of, and report to, the GSIS Board of Trustees.

The ROC reports to the Board its annual accomplishment through the submission of a Committee Report. (n)

The ROC, through its Secretariat, shall maintain appropriate records of its deliberations and decisions (minutes of meetings, directives, and resolutions). Such records shall document the ROC's fulfillment of its responsibilities and facilitate the assessment of the effective performance of its functions. (n)

3. MEMBERSHIP

All Trustees are members of the ROC.

The ROC Chairperson should have *risk management*, finance, or investment background. (r)

The ROC Chairperson shall be selected by a majority of the members present in a Board Meeting *called for that purpose* upon reaching a

quorum. (r)

4. MEETINGS

The ROC shall meet at least once a month or *more frequently as may be necessary.* (r)

The presence of a majority of incumbent Trustees shall constitute a quorum, where majority is defined as 50% of the total number of incumbent Trustees plus one (1).

Meetings may be conducted or members may participate in the meetings via physical attendance, teleconference, videoconference, or other virtual means capable of recording and recognizing the participation of the members and of recording and storing the proceedings of such meetings, including the date and time of meeting. (r)

5. SCOPE OF AUTHORITY

5.1 Review and evaluate proposed policies on risk identification, measurement, and monitoring methods or instruments for the risk management program in accordance with international standards, with technical assistance from consultants when necessary.

5.2 In line with its policy-making and oversight functions, the ROC shall have the authority to obtain assistance from all units of the System and other consultants in carrying out its functions. The ROC shall likewise have the authority to direct the Legal Services Group to conduct investigations on any matter within the scope of the ROC's responsibilities.

5.3 *Require fund managers, both local and international, to regularly report the status and performance of funds or assets under management.* (n)

5.4 *Exercise functional authority over the Risk Management Office (RMO) and evaluate, review, or rate annually the performance of the RMO and the head of the RMO.*

5.5 Require the RMO to regularly report the results of its risk monitoring on all Financial and Operational Risks, its recommendations thereto,

n – new provision
r - revised provision

and the appropriate actions taken by Management. *(previously part of the section on Reporting)*

5.6 *Require the RMO to submit risk analysis of all matters that will be taken up in ROC meetings.* (n)

5.7 *Review the business cases for new projects, programs, and activities of RMO, Information Technology Services Group, Information Security Office, Financial Management Group, Insurance Group, Real Estate Asset Disposition and Management Office, and Actuarial and Risk Management Group.* (n)

5.8 Review policies and procedural guidelines pertaining to new loan and insurance products, investment guidelines, and such other related policies.

5.9 Review and evaluate all IT-related projects and technology architecture decisions by requiring the submission of the appropriate reports and documents as may be deemed necessary by the ROC. (r)

5.10 Require the Chief Information Officer and the Chief Security Officer to regularly report the status *and submit post-implementation review* of all IT and information security-related projects. *(previously part of the section on Reporting)*

5.11 Require Management to submit risk reports such as those pertaining to investment properties, market, financial, credit, regulatory, and such other risks as may affect GSIS.

5.12 *Require the reporting of all other risk-related matters and issues.*(n)

5.13 Request, through the Office of the President and General Manager (OPGM), GSIS officers and employees to attend its meetings and to provide information and/or assistance as may be necessary.

6. FUNCTIONS AND RESPONSIBILITIES

The ROC's functions and responsibilities are to set risk policies and oversee System-wide risks to assure their consistency with the strategy and business objectives of the System.

Meanwhile, the Board delegates to Management the tasks of accepting,

n – new provision
r - revised provision

controlling, and monitoring specific risks.

6.1. Overall Responsibility of the ROC:

a. To review the System's risk policies, including System- wide risk limits, for evaluation and approval of the Board;

b. To review risk-related aspects of specific proposals submitted to the Board for approval;

c. To proactively assess the likely impact of key risks on the future institutional viability of the System, based on established risk appetite, which can be a basis for the Board to require Management to plan mitigating and suitable responses as well as institute controls; and

d. To undertake any activity that may be required by the Board in the area of risk identification, assessment, and monitoring.

6.2 *Ensures that the Enterprise Risk Management Framework is implemented within the organization.* (n)

a. *Monitor compliance with* risk acceptance criteria for identified key risks to be implemented by Management. (r)

b. Evaluate System-wide risk scenarios through the reports to be submitted by the RMO.

6.3 Review and recommend to the Board of Trustees risk policies consisting of:

a. A concise statement of risk policies;

b. A structure of established risk limits and the corresponding guidelines for risk acceptance by Management;

c. An accurate register of System-wide risk information including an effective tool for gathering, storing and consolidating risk reports; and

d. A comprehensive system for monitoring compliance by

n – new provision
r - revised provision

Management to established risk exposures.

6.4 Evaluate GSIS-wide risk policies and implementation of Management's strategies and plans.

6.5 Build risk awareness and strengthen support structures for risk oversight

a. Promote a culture of risk awareness between the Board of Trustees and top Management through communication and updates on risk issues, guidelines, and information on policies and System-wide risk scenarios.

b. Require or direct the RMO to:

1. Develop and improve systems that support risk management, e.g., improving the quality of records and use of information technology for oversight reports;
2. Analyze gathered data;
3. Give scenarios as to the risk effect; and
4. Give recommendation/s based on the analysis and risk scenario effects.

6.6 Oversee All IT Matters and Concerns

6.6.1 IT Projects

a. Appraise and critically review the financial, tactical, and strategic benefits of proposed major IT-related projects and technology architecture alternatives.

b. Appraise and critically review the progress of major IT-related projects and technology architecture decisions.

c. Make recommendations to the Board of Trustees with respect to IT-related projects and investments that require Board approval.

6.6.2 IT Security

a. Monitor the quality and effectiveness of the System's IT

security.

b. Periodically review and appraise the System's IT disaster recovery capabilities.

6.6.3 Internal Controls

a. Monitor the quality and effectiveness of IT systems and processes that relate to or affect the System's internal control systems.

b. Monitor and assess the System's management of IT-related compliance risks, including IT-related internal audits.

6.6.4 Others

a. Perform such other duties as are necessary and appropriate to ensure that the System's IT programs are effectively supporting its business objectives and strategies, or as the Board may direct.

b. Coordinate with the Audit Committee regarding IT systems and processes that relate to or affect the System's internal control systems.

7. CHARTER REVIEW

The ROC shall assess the adequacy of this Charter every year, or as often as may be necessary, and recommend to the Board amendments and updates whenever there are significant changes therein. (r)

n – new provision
r - revised provision