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

RISK MANAGEMENT PROGRAM

I. Risk Management in the GSIS

The GSIS has established an Enterprise Risk Management (ERM) System to ensure that assets are managed properly and that quality service is rendered to all stakeholders of the GSIS. Using an ERM framework, GSIS observes a system-wide and integrated approach to risk management to enhance governance and compliance mechanisms and effectively identify, assess, manage, and report risks. Groups, offices, and departments pursue risk management at the business levels and within the context of the whole organization in order to have a cross-cutting, enterprise-wide view of risks.

The GSIS Board of Trustees recognizes that risk management is an important component of the over-all management of the GSIS. The Risk Oversight Committee (ROC) of the Board assists the Board of Trustees in its policy and oversight functions by formulating risk policies, setting System-wide risk limits, and reviewing the risks and rewards balance of specific proposals.

As proof of the importance of risk management in the organization, the GSIS Board of Trustees has placed the establishment of a robust enterprise-wide risk management system front and center of the GSIS Strategy Map. It is therefore necessary for risk management in GSIS to be overseen and coordinated by a distinct office, the Risk Management Office (RMO) to drive the process. In 2017, to further strengthen risk management and corporate governance, the RMO was transferred from the Actuarial and Risk Management Group to the Research, Innovation, and Strategic Advisory Sector, and functionally under the ROC.

The President and General Manager as Chief Executive Officer leads the risk management campaign by translating strategic objectives, policies, and guidelines emanating from the Board of Trustees into implementable plans, projects, procedures or processes to be executed by the different levels of management. This ensures that risk management is applied to the setting of strategy, the achievement of objectives, and the conduct of operations. The PGM oversees the observance of GSIS-wide risk policies and implementation of management strategies and plans and prioritizes the treatment of certain risks.

The RMO, with engagement from management, drives the enterprise risk management program. It leads the process to conduct risk and opportunity and control assessment exercises, updating risk registers and heat maps. The output of the risk and control assessments, consultations, and group discussions are used as sources for the system-wide risk assessment and identification of GSIS key and priority risks. Controls are identified and assessed relative to these key risks. Key risk indicators are identified based on available data from the functional groups; these serve to measure and monitor risks, and the status of these risks are communicated in risk monitoring reports to Management

and the Board. Groups, offices, and departments are encouraged to continually identify emerging risks and report them to the RMO as they surface.

GSIS devised an experimental risk maturity assessment test based on existing models at the time to measure its own ERM progress. This is in preparation for a possible future third-party objective assessment. To determine the ERM maturity rating for each year, RMO conducts an enterprise risk maturity assessment survey for the Board of Trustees and GSIS executives as respondents.

Risk appetite statements have been drawn up to establish the standpoints of the Board and GSIS on various areas of concerns. These attempt to highlight key elements in GSIS's risk governance and reporting framework and are established by the Board of Trustees to articulate the nature and extent of principal risks that the organization would be willing to take to achieve strategic objectives. Corollary to this, risk alert triggers and thresholds have been defined that provide targets, tolerance thresholds, and limits to ensure that decisions and actions are aligned with the over-all risk appetites and tolerances.

GSIS has successfully been awarded several ISO Quality Management System certifications which attest to the risk management practice and risk-based thinking mechanisms in GSIS in the pursuit of quality service for its customers.

II. GSIS Key Risks and Control Measures

Among the operational risks which GSIS focuses on are those that are related to the integrity and availability of data and information, internal business processes, business continuity and resilience, IT risks. GSIS controls and mitigates these operational risks so that material damage is avoided or remain under manageable levels.

- Information Integrity Risk

  This is the risk on accuracy, completeness, consistency, reliability, and timeliness of both internal and external information. Information integrity may be broadly defined as the trustworthiness and dependability of information content, processes and systems.

  Erroneous data and information, and delayed submission of data from external sources, i.e. the agencies which are responsible for remitting premium and loan payments of members can result to issues of mismatch with the membership database. GSIS utilizes data from other government agencies for updating the service records and salary information of employees. The data is used to process claim applications for loans, retirement, separation benefits, policy maturity, and other benefits. The discrepancies in the data bases could result in incorrect computations and delays in the processing of claims as these would necessitate re-work to reconcile the data.

  In order to mitigate these data matching issues, the eBilling and Collection System (eBCS) aims to put GSIS a step closer to reducing the number of data entries for clarification at the data source, which are the remitting agencies. The project utilizes advanced internet-based technologies, which would allow two of more computer devices to communicate over a network. The system provides remitting agencies with

automated means to ensure that corrections and updates have been made before the payment data enters the GSIS database.

- Process Risk

  This is when enterprise processes do not fully address the requirements of customers and the business; when processes seem unresponsive to needs, inconsistent or inflexible, not in accordance with standards or service level commitments. Losses could occur due to inappropriate or faulty design of processes.

  For example, a key risk indicator for process risk is Turn-Around Times for Claims Processing. Delays in the release of benefits or claims can be a cause for member complaints and dissatisfaction.

  The turnaround times (TAT) for mandated services of GSIS to its members and pensioners such as claims on retirement, life insurance, funeral benefits, among others benefits are given attention and monitored regularly for compliance. This monitoring has influenced the performance of GSIS such that benchmarks for measuring TATS were met. Performance bars were elevated, resulting to better overall customer satisfaction.

- Business Disruption

  Risks of disruptions could entail the failure to resume business operations, deliver services, establish communications, and access critical systems during or in the immediate aftermath of a natural or man-made disaster.

  Business Continuity Plans (BCP) for Mission-Essential Functions have been prepared for the GSIS Head Office and Branch Offices under the guidance of the RMO with cooperation from the different Functional Groups and process owners. The business continuity plans are operational guides for process owners on how to respond to business disruptions that may affect mission-critical or mission-essential functions of GSIS.

  The BCPs are to be activated when services and operations in the GSIS Head Office and Branch Offices are seriously compromised and/or exposed to risks over a period time, thus necessitating the use of alternate sites, process-transfers, or work-from-home or work-offsite strategies. Business Continuity Teams for different mission-essential functions have been set up. The different business continuity management systems such as the Disaster Contingency Committee, the Crisis Communication Team, the IT Disaster Recovery and Management Team, the Emergency Response Team, and Business Continuity Teams led by RMO work together to make the GSIS more resilient and responsive.

- Systems Failure and Disaster Recovery

  To ensure that data is not lost when critical issues arise, all managed database, business system data, and configuration information are backed up on a regular basis. The GSIS has alternative recovery programs and backup systems. Recovery tests are conducted to examine all backup processes, procedures as well as the integrity of

back-up information. To do these, GSIS has its IT Disaster Recovery and Management Team.

- Technology Risks

  The IT Steering Committee reviews and recommends to the President and General Manager and/or the Board of Trustees IT-related proposals. It evaluates and prioritizes IT-related policies, plans and initiatives. It serves as a review body for all IT programs and projects and the clearing house for the procurement of IT-related goods and services and acquisitions. The Committee helps the PGM and BOT manage the risks and address significant IT-related issues.

The nature of GSIS operations inevitably involves financial risks that must be measured, monitored and managed by an effective risk management system. Effective risk management ensures that operational as well as financial risks are properly identified, assessed, measured, and managed overall. The diligent monitoring and management of risks require the development of a risk-conscious culture that will influence daily business activities and decision-making.

In the management of financial risks, the Risk Oversight Committee (ROC) and Assets and Liabilities Committee (ALCO) assist the Board of Trustees and the President and General Manager. The ALCO's functions are to ensure the efficient implementation of balance sheet management policies; review, assess, and recommend new loan products and investment proposals; recommend the strategic asset allocation according to risk appetite; review financial performance versus targets.

- Market Risk

  Market risk is the risk that the value of an investment will fluctuate due to changes in market factors, such as foreign exchange rates, interest rates and other factors that relate to market volatilities on the rate, index or price of the underlying financial instrument. Sensitivity analysis is a technique used to quantify the effects of these volatilities on the financial instrument, thereby providing a measure for market risk.

  To manage market risk, the GSIS is guided by the Investment Policy Guidelines (IPG), which promotes the safety of the funds, optimizes the returns on its investments, and satisfies the liquidity requirements of the System. The IPG aims to define the types of investments and transactions that the fund may invest in, provide a framework for managing the risk of the portfolio, and incorporate best practices in the management of investments.

  GSIS also monitors investment risk by conducting risk assessments of its investment transactions and prepares monthly financial risk monitoring reports, which include Value-At-Risk (VAR) analysis and stress tests on the GSIS portfolio of securities.

- Credit Risk

  Credit risk is the risk of financial loss arising from the counterparties' inability or unwillingness to settle their financial obligations to the GSIS as expected or originally contracted. To manage credit risks for its loans to members, the GSIS carefully sets, and constantly monitors and assesses the terms and conditions of member loan programs. This ensures that the programs remain financially viable for the GSIS, responsive to changing market conditions, and suited to members' requirements.

  Aside from credit risk arising from loans to members, GSIS is exposed to credit risks from its holdings of fixed income securities and equities. To manage counterparty risks, the GSIS is governed by the Counterparty and Issuer Risk Guidelines (CIRG). The CIRG provides a framework to manage the credit risk exposures of GSIS to counterparties in transactions affecting the investment of funds and to issuers of securities taken into the investment portfolio.

- Liquidity Risk

  Liquidity risk is the risk that the available cash and current collections of the GSIS will be unable to fund short-term obligations as they fall due, and when the GSIS encounters difficulty in realizing its assets and raising funds to meet those financial liabilities.

  GSIS manages this risk through the daily monitoring of cash flows, taking into account due dates on future payments and daily collection amounts. GSIS also maintains a sufficient portfolio of highly liquid assets that can be easily converted to cash as protection against unforeseen disruptions to cash flows. GSIS is also able to dispose of investments which are actively traded in the market, including publicly traded equity, high-yield short-term placements (HYSTP), and marketable bonds.

  In its continuing pursuit to address fund management and investment risks, GSIS intends to rationalize its policies and procedural guidelines. For example, in trading and investment activities, rules and protocols are continuously being evaluated, while cut-loss limits and trailing stops in equity trading will be implemented. At the same time, a more risk-based and system-wide approach will involve adopting integrated systems that interface seamlessly among the treasury, accounting, and trading (front desk) functions.

- Insurance Risk

  Insurance risk is the likelihood that an insured event will occur, requiring the insurer to pay a claim to the insured. Insurance companies compensate for this risk by adjusting premiums according to how great the risk is.

  The GSIS, by virtue of Republic Act 656 and as amended by Presidential Decree 245, is mandated to insure all properties, assets, and interests of the government against any insurable risk. All government involvement or exposure in corporations, partnerships, joint ventures, associations, and the like are regarded as government interest and it is mandatory for them to obtain their insurances and bonds from GSIS. The GSIS offers various non-life insurance products that provide protection to both institutional and individual clients. To institutional clients, GSIS offers non-life

insurance coverage such as fire, engineering, marine hull and cargo, aviation, contractor's all risk, bonds, motor car, and personal accident. For individual clients, including GSIS members, pensioners and their dependents, the pension fund offers optional life and non-life products as part of its mandate to issue all forms of non-life insurance.

While the GSIS creates value for the General Insurance Fund (GIF) with cash inflows composed of premiums, investment income, reinsurance contribution, and recoveries, it has to maximize these against outflows of claims and reinsurance cession. To address the risk of substantial claims losses, GSIS passes significant portions of its exposures to reinsurance companies. These reinsurance companies assume the risks and enjoy the premiums that are passed on by the GSIS.

The Underwriting Department of the Insurance Group perform reviews and evaluations of claims losses as risk-mitigating measure particularly for substantial claims. The agencies' loss history over a five-year period, including other factors are reviewed to explore the possibility of raising premium rates. Risk inspections are also conducted from time to time, with recommendations depending on the size and importance of the account.

In addition, in order to mitigate the risk of GSIS exposure to extreme losses with regard to its retained portion, the GSIS procures a Property and Engineering Excess of Loss Coverage. This ensures that GSIS is also protected with regard to its retained portion for its property and engineering coverage.