



SSS Risk Oversight

Under its Resolution No. 887 dated 27 November 2019, the Social Security Commission (SSC) approved the Report on the Risk Management and Risk Oversight which provides an assessment of the adequacy of the risk management system in the Social Security System (SSS), as endorsed by the Risk Management and Investments Committee.

Current Risk Management System in place. The Enterprise Risk Management (ERM) in the SSS, a holistic approach to risk management, was implemented which focuses on the following key components: (1) Corporate Governance; (2) Line Management; (3) Portfolio Management; (4) Risk Transfer; (5) Risk Analytics; (6) Data and Technology Resources; and (7) Stakeholders Management. The ERM Framework, to ensure the adoption of adequate and effective enterprise-wide risk management system, and the ERM Policy, to ensure adherence to best practices in the identification, analysis, estimation and evaluation of risks, were also developed to support the ERM.

How are key risks being managed? In managing risks, effective measures were established under the following risk categories: (1) Financial Risks - whereby a Risk Dashboard was developed to identify the financial risks and other financial-related risks, e.g., market, credit and liquidity, that SSS is facing and ensure adherence to the provisions of SSS Law, Policies and Guidelines in Determining and Managing Exposure Limits to Debt and Equity and stock accreditation guidelines; (2) Insurance and Demographic Risks - through conduct of actuarial valuation/studies and monitoring of experience; (3) Strategic Risks - through monitoring new and pending bills, conduct of regular economic researches/studies, implementation of the No Gift Policy, No Noon Break Policy, Anti-Fixer Campaign and No Smoking Campaign; and (4) Operational Risks - through conduct of regular Risk and Control Self-Assessment through the system and application of the tools to address the operations risks, such as: (a) Privacy Impact Assessment; (b) Personal Equity Investment Policy; and (c) Business Continuity Management Program.