ENTERPRISE RISK MANAGEMENT (ERM)

SMIC's Enterprise Risk Management approach begins with the identification of risks, followed by the assessment of risk interrelationships and analysis of risk sources. This is followed by the development of risk management strategies and action plans, and ultimately, the monitoring and continuous improvement of the risk management process.

SMIC's business unit heads are responsible for managing operational risks by implementing internal controls within their respective units. The Risk Management Committee is regularly updated on the Company's risk management systems, as well as on improvement plans of SMIC, while the Executive Committee provides oversight on the assessments of the impact of risks on the strategic and long-term goals of the Company.

Actions adopted to mitigate the Company's risks include investment in technology, the provision of continuous training to personnel, the performance of regular audit and the establishment and implementation of policies for strong Information Technology (IT) governance, and continued partnership with the Company's various stakeholders.

Technological risks are addressed via continuous risk assessments, wherein potential threats to assets, vulnerabilities and likelihood of occurrence are evaluated and possible impacts are estimated in the area of networks, operation systems, application and databases in production. Specifically, system vulnerability assessments are regularly conducted to proactively detect and address threats.

The Company's approach to other risks, like environmental risk starts with an assessment of the potential impact it has to the community where it operates. There is a regular reporting of the group's sustainability road map and progress. The Company is committed to protect the environment by implementing effective and efficient resource utilization measures in its daily operations.

RISK EXPOSURES AND CONTROL MEASURES

Risk Categories	Risk Management and Controls
Financial Risk	• Regular monitoring of interest rates, Forex rates, and financial ratios. • Please refer to Financial Risk Management Objectives and Policies on Note 27 of the Notes to Consolidated Financial Statements on pages 71 -76 found in the Annual Report as of Dec 31, 2021 and Definitive Information Statement for the Year ended Dec 31, 2021. https://www.sminvestments.com/about-us/governance/disclosure-transparency/
Operational Risk - Safety and Security	• Annual audit of the SM Group Safety and Security Team which include among others, the safety protocols within the perimeter, CCTV, etc. With the Pandemic, strict health protocols are being checked for compliance regularly to ensure that it is in line with the Department of Health (DOH) and Inter Agency Task Force (IATF) guidelines of the government. • Results of the audit are validated and monitored by SMIC Internal Audit Team. • Department personnel are also trained to respond to safety and security incidents. • Implemented an efficient SMS blast technology for easy communication in case of an emergency. With the Pandemic, the usage of the tool was maximized as this is being used to disseminate information and provide instructions to all employees. • SMIC ensures proper maintenance of facilities to minimize the impact of physical security risks which may affect its operations.
- Property Damage and Business Disruption	• Annual review of Business Continuity Program and business impact assessment. • SMIC continues to improve its Business Continuity Management System through the implementation of regular data back-up procedures and maintenance of a Disaster Recovery site to ensure the availability of critical resources and information assets anytime.

	• The Company undergoes at least twice a year business continuity exercises that are reported to the Board Risk Committee. • With the Pandemic, the Company is able to invoke and make use of the Business continuity plan and business operations is not affected much. Ability and flexibility to work from home condition is made possible with strong security measures in place.
Technological Risk - Cybersecurity	• Conduct vulnerability assessment and penetration testing and incident reporting. In 2019, SMIC engaged the service of SGV & Co. to perform an independent assessment. • Cybersecurity training across the business units to address the human factor in cyber security management. • SMIC also adopt the latest IT tools and technology to combat cybersecurity threats that may impact operations. • Organized a team of IT professional with expertise in information security that monitors, analyzes and protects the company from cyber-attacks.
Environmental Risk	• Regular reporting of the group's sustainability road map and progress. • SMIC is committed to protect the environment where it operates by implementing effective and efficient resource utilization measures in its daily operations. • SMIC is fully committed in reducing its carbon footprint, the company recycles its waste, conserves water and harnesses renewable sources of energy. SMIC also supports several initiatives by the SM Foundation in its sustainability programs. • SMIC is also committed in promoting equal opportunities for persons with special needs, senior citizens, women and indigenous people.
Regulatory/Compliance Risk - Data Privacy Act (DPA)	• SMIC conducts regular employee awareness on Code of Ethics, Data Privacy Act of 2012, and other external regulations through constant training of personnel to ensure its mandatory and consistent compliance.

	• Develops e-learning tools on various topics for easy tracking of employees training progress. Even during the Pandemic, the Company is able to sustain the training needs of the employees utilizing the online platform. • There is a continuous monitoring of the data privacy compliance especially on contact tracing forms and apps. • Privacy Impact Assessment (PIA) is prepared for new systems, processes and programs that involve personal information. • Sharing of personal information with other parties or any services being outsourced to outside parties are adequately covered with a DPA agreement.
- Anti-Money Laundering/ Counter Terrorism Financing	• Registered with Anti-Money Laundering Council (AMLC) last December 1, 2021 as Designated Non-Financial Business and Profession (DNFBP). Certificate of Registration (COR) was awarded last March 31, 2022. • All Board members and Key officers underwent seminars/training on Anti-Money Laundering Act (AMLA) provided by an accredited AMLC service providers to ensure understanding of the implementing rules and regulations of the Act for an effective implementation. • A risk-based Money Laundering/Terrorism Financing Prevention Program (MTPP) was developed and approved by the Board on March 14, 2022, which detailed the procedures and implementation of the major requirements of AMLA.

RISK MANAGEMENT FRAMEWORK

SMIC uses this framework/process to identify potential threats to the organization and/ or departments' goals and objectives, and to define the strategy for eliminating or minimizing the impact of these risks, as well as the mechanisms to effectively monitor and evaluate the strategy.	
Steps	**Tasks Description**
1. Event or Risk Identification	To identify units of risk, threats and opportunities within the department or business units.
2. Risk Assessment	To evaluate the risk identified, i.e., the likelihood for the risk to happen, impact it may have to the organization or business unit/departments and the cost of the risk.
3. Risk Response	To determine the risk treatment whether to accept the risk, avoid the risk, transfer the risk or mitigate the risk identified.
4. Review/Verify Control Functions	To define the strategy or controls to minimize or eliminate the impact of the risks.
5. Information and communication	To disseminate information for stakeholders' participation and commitment with regards to the risk identified.
6. Monitoring	To establish measures and protocols for continuous improvement.