ENTERPRISE RISK MANAGEMENT (ERM)

SMIC's ERM 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 evaluation 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.

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 Information Statement and Notice of 2020 ASM page 71-76 https://www.sminvestments.com/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. • 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. • 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.
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.
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	• 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.

RISK MANAGEMENT FRAMEWORK

SMIC used 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.

1. Event or Risk identification – identify units of risk, threats and opportunities.
2. Risk Assessment – evaluate the risk identified (i.e., likelihood to happen, impact to the organization or department and cost of risk.)
3. Risk Response – determine risk treatment (i.e., accept, avoid, transfer, mitigate)
4. Control Activities – define the strategy or controls to minimize or eliminate the impact of the risks.
5. Information and communication – disseminate information for stakeholders' participation and commitment.
6. Monitoring - establish measures and protocols for continuous improvement.