

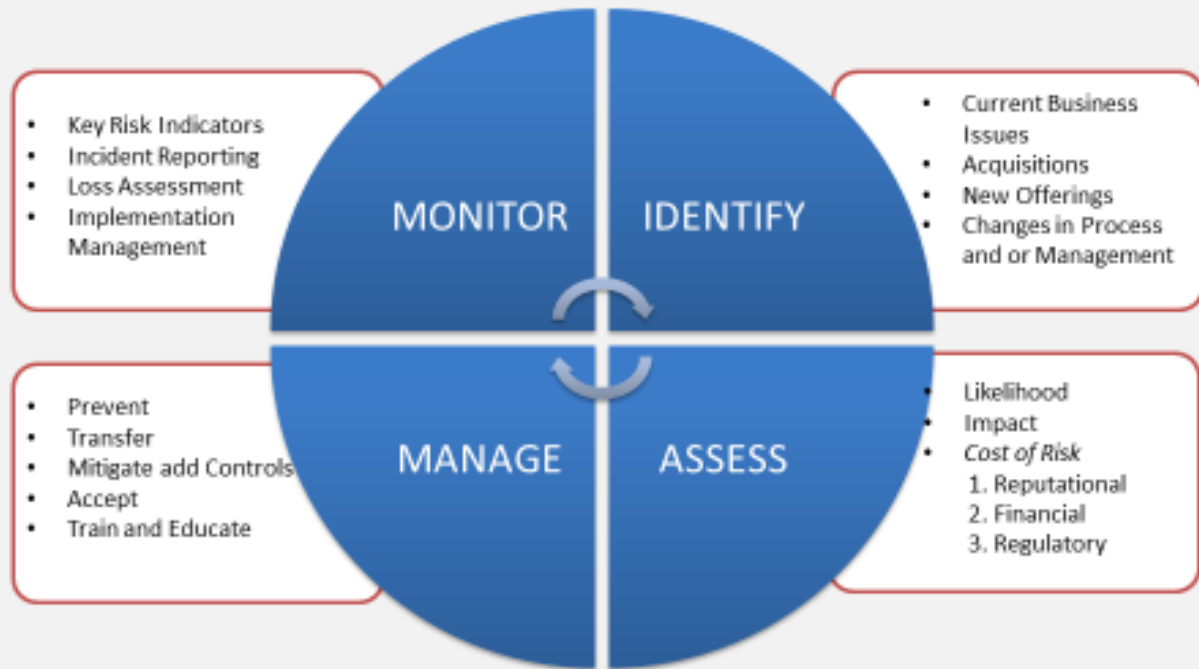
## ***Enterprise Risk Management (ERM)***

SMIC's ERM approach begins with the identification and prioritization 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 assessment 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 audits, the establishment and implementation of policies for strong information technology (IT) governance, and continued partnerships 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 areas of networks, operating systems, applications and databases in production. Specifically, system vulnerability assessments are regularly conducted to proactively detect and address threats.

# RISK MANAGEMENT CYCLE



Risk Exposure	Risk Assessment (Constant Monitoring and Measurement Process)	Risk Management and Control (Structures, Procedures, Actions Taken)
<b>Safety and Security Risk</b>	<p>Annual audit of the SM Group Safety and Security Team.</p> <p>Results of the audit are validated and monitored by the SMIC Internal Audit Team.</p>	<p>Department personnel are also trained to respond to safety and security incidents.</p> <p>SMIC ensures proper maintenance of facilities to minimize the impact of physical security risks which may affect its operations.</p>
<b>Property Damage and Business Disruption Risk</b>	<p>Annual review of business continuity and Business impact assessment.</p>	<p>SMIC continues to improve its Business Continuity Management System (BCMS) through implementation of data back-up procedures to ensure availability of critical resources.</p> <p>The Company undergoes an annual business continuity exercise that is reported to the Risk Committee.</p>
<b>Information Security and Technology Risks</b>	<p>Vulnerability assessment and penetration testing, incident monitoring</p>	<p>The Information Security Department monitors the compliance of the Information Security Policy and incidents of any system security breaches.</p> <p>SMIC through the course of the year conducts Information Security Awareness and Cyber Security Risk Management training across the business units to address the human factor in cyber security management.</p> <p>SMIC also endeavors to use the latest sophisticated technology to combat cybersecurity threats that may impact operations.</p>
<b>Environmental Risk and Social Risk</b>	<p>Regular reporting of the group's sustainability road map and progress</p>	<p>SMIC is committed to protect the environment where it operates by implementing effective and efficient resource utilization measures in its daily operations.</p> <p>SMIC through its partnership with SM Foundation reduces its consumption, recycles its water and wastes and harnesses renewable sources of energy.</p> <p>SMIC is also committed in promoting equal opportunities for persons with special needs, senior citizens, women and indigenous people.</p>

Risk Exposure	Risk Assessment (Constant Monitoring and Measurement Process)	Risk Management and Control (Structures, Procedures, Actions Taken)
<b>Operational / Process Risk</b>	Business process reviews	<p>The Risk Management Team reviews business processes and initiates the creation of tools and or procedures that enhance operational efficiency.</p> <p>The Company continues to improve on its business processes to ensure operational efficiency of all the Business Units.</p>
<b>Financial Risk</b>	Regular monitoring of interest and forex rates, financial ratios.	Please refer to the Company's 2017 Annual Report pg. 117.
<b>Regulatory and Compliance Risk</b>	Compliance monitoring and reporting	SMIC conducts regular employee awareness and mandatory compliance to the Code of Ethics, Data Privacy Act and other external regulations through constant monitoring and training of personnel.