Emerging Risk Management

The Company has monitored both internal and external conditions to pinpoint emerging risks that may disrupt and affect the operations. Climate change and advancement of technology are considered two emerging risks that require preventive and adaptation measures. The measures are summarized as follows:

Risk factor	Risk driver	Control and management method
Climate Change Risk level : Medium	• Increasing frequency and severity of natural disasters. • International efforts to limit the use of coal and fossil fuels in electricity generation, in order to reduce carbon emissions and keep global temperatures from exceeding 1.5 degrees Celcius. • Regulatory actions to control carbon emissions, for example via carbon tax.	• Prepare the Climate Change Strategy and study greenhouse gas emission management and reduction approaches for the setting of emission targets to achieve carbon neutrality in 2050. • Set the target to raise renewable energy capacity to at least 25% of total capacity within 2025. • Invest more in energy-related technology and innovation that supports carbon neutrality / Net Zero target. • Promote reforestation and forest conservation for carbon sequestration. • Require power plants to prepare GHG inventory and estimate carbon footprints, for the formulation of GHG management and emission reduction plan and targets. • Study carbon credit trading, carbon pricing and carbon offsetting mechanisms.
Human Rights Risk Risk level : Low	• Exposure in various businesses in several countries involves a great number of direct and indirect stakeholders from employees, suppliers and partners to community and a chance of operational impacts on these stakeholder groups.	• Constantly monitor the compliance with the Human Rights Policy and the Supplier Code of Conduct. • Constantly conduct human rights risks and impacts assessment; set preventive and mitigating measures; and prepare the compensation and remediation process in line with international standards. • Constantly assess safety and occupational health risks; and review safety measures for employees, suppliers, sub-contractors and community.
Cybersecurity Threat	• Rapid development of information technology and IT	• Set security measures for essential IT systems concerning the backup system, password setting, identity authentication, etc.

Risk level : Low	systems that underpin business operations. • Digital transformation leading to possible breach, theft or destruction of information that endangers operation/business continuity.	– Set IT risk management guidelines, define the duties of individuals responsible for IT risk management; and prepare the system recovery plan. – Assess cybersecurity risks in line with international standards, constantly test the system and set necessary measures to close the gaps.

Crisis and business continuity management

RATCH has the Business Continuity Plan and the Crisis Management Plan, to contain the impacts from controllable yet unpredictable crises that may be originated internally or externally. The plans are to ensure business continuity. Both plans have been integrated into the Emergency Response Plan of RATCH and all subsidiaries and joint ventures, for more streamlined actions and management efficiency. The procedures and actions as well as emergency situations in all plans are reviewed on an annual basis.

Business Continuity Management Policy