Type of Risk and Management Method

Risk Management Department identified several strategic risks that impact Telkom's business activities, including:

Type of Risk	Risk that is Faced	Impact to Telkom	Mitigation/Risk Management
1. Systemic Risk			
Political and Social	Disruptions to political stability, social, and security turmoil both domestically and internationally caused by specific issues such as geopolitical crises, trade wars, and so on.	It has a negative impact on business growth, operations, financial condition, results of operations, supply chain of production equipment and prospects, as well as market prices of securities.	• Monitoring the influence of socio-political turmoil on operational/service disruptions. • The maintenance of awareness through the improvement of safety & security functions. • Monitoring supply chain issues related to raw materials and looking for alternatives to materials/device designs.
Macro Economy	• Changes in the rate of inflation. • The fluctuation of Rupiah exchange rate. • Increase in energy and fuel prices. • Increase in loan interest rates. • The decrease of government or company's credit rating.	• Affects the purchasing power and ability to pay customers. • Have the impact on the business, financial condition, business result or business prospect. • Have a material adverse effect to the business, financial, condition, business proceeds or business prospect.	• Monitoring of the influence of macroeconomy to the change to increase the expense through Cost Leadership program. • Maintain healthy financial ratio to get competitive interest rates. • Loan restructuring with less competitive interest rates. • Maintain sufficient foreign currency asset according to business needs.
Risk of Disaster and Epidemic	Natural disasters such as hurricane, earthquake, tsunami, volcanic eruption, fire, drought, endemic, and pandemic.	Disrupting its business operations and give negative impact to the financial performance and profit, business prospect as well as market price of securities.	• Monitoring indicators that have the potential to cause disturbances to equipment such as device humidity and temperature, ship traffic on the SKKL route through the system. • Transfer of risk by using the insurance of asset to anticipate the natural disaster and fire. • Coordination with ASKALSI (Indonesian Sea Cable Association) and BAKAMLA (Indonesian Marine Safety Agency) to secure SKKL. • Preventive & corrective action by preparing the disaster recovery plan and crisis management team.

Type of Risk	Risk that is Faced	Impact to Telkom	Mitigation/Risk Management
Risk of Climate Change	Unpreparedness to respond to climate-related risk is driving extreme weather event such as flood, and long-term change in climate pattern such as rising temperature.	Damage to network asset and infrastructure, operational disruption including on-grid power outage, decreased employee productivity due to disruption to transportation or site access, and safety threat to field employee.	• Upgrade infrastructure to increase resilience to climate change-induced disaster. • Have Business Continuity Management procedure and disaster management guideline. • Mitigate the risk of overheating by ensuring the building has optimal cooling condition. • Establish GHG emission reduction initiative. • Carbon-offset program through reforestation and conservation effort, utilization of renewable energy and energy efficiency. • The Energy Efficiency Awareness Movement (GePEE) is implemented in all office buildings and Plazas.
2. Business Related Risks			
Operational Risk	The failure in the sustainability of network operation, main system, gateway on Telkom's network, or other operator's network.	It has a negative impact to the business, financial condition, proceeds from the operation and business prospect.	• Implementation of BCM, BCP, and DRP. • Integrated Management System (IMS) Certification for infrastructure management.
	Physical security threats such as theft, vandalism, riot, terrorist attack that are beyond Telkom's control or other actions as well as cyber security threats such as brute force attack, DDoS attack, and threat in Data Center.	Has the negative impact to the business, financial condition, result from the operation materially.	• The upgrade of preventive action in the form of vulnerability assessment and penetration test periodically. • Monitor and identify all types of attack in the real-time as well as to choose and conduct the necessary action immediately. • Preparing the recommendation to handle cyber-attack based on the historical incident analysis. • Intensive coordination with relevant parties to handle the cyber-attack. • Monitor the situation and coordinate with relevant law enforcement officer (e.g., Police) to maintain the security of asset and building.

Type of Risk	Risk that is Faced	Impact to Telkom	Mitigation/Risk Management
	Delay in adoption of new technology.	Negative impact on competitiveness.	• Preparation of a technology roadmap by considering future technology and potential implementation of competitor technology. • High-Level-Design (HLD) evaluation and validation through LAN simulation to check interoperability between platform.
Financial Risk	Credit risk mainly comes from trade receivable and other receivable.	Have an adverse impact on financial condition, operational performance, and business prospect.	• Continuous monitoring of account receivable balance and carrying out regular collection effort.
	Liquidity risk.	Impact on the ability to meet financial liability, when these financial liabilities fall due.	• Preparation of a technology roadmap by considering future technology and potential implementation of competitor technology. • Conduct analysis to monitor the liquidity ratios of the financial position statement such as the current ratio and debt to equity ratio against the requirements required by the debt agreement.
	Limitation in finding funding source for investment initiative.	Have a material adverse impact on the business, financial condition, operational performance, and business prospect.	• Maintain and improve company performance to gain trust from national and global funding institution/source.
Legal and Compliance Risk	Civil lawsuit and/or breach of contract from third party (vendor, partner or cooperation partner).	Reduce Telkom's revenue and negative impact on business, reputation, and profit.	• Strengthening legal review of contract document with third party and monitoring the settlement of right and obligation according to the contract. • Strengthening internal policy related to procurement and cooperation process.
	Personal data leak.	A maximum fine of 2% of income based on regulation on personal data protection.	• Program to increase employee awareness of personal data protection regulation. • Supervision and evaluation of data transaction mechanism and implementation within the company. • Strengthening cyber security to ensure protection of personal data managed in the company.

Type of Risk	Risk that is Faced	Impact to Telkom	Mitigation/Risk Management
Regulation Risk	The change of Indonesian or International regulation.	Has the impact to the business, financial condition, operational performance, and business prospect.	• Analysis on the impact of the regulation plan towards the industry in general and Telkom in particular. • Giving inputs so that the regulation that will be stipulated will give positive impact to the company and industry.
Transformation Risk	The failure of significant business and organizational transformation initiatives.	Has an impact on business growth and the company's financial performance in the short and long-term.	• Preparation of strategic fit and roadmap for transformation initiative. • Conduct risk assessment on transformation initiative both at the pre- and post-transformation stage (including ensuring that customer service continue to run). • Implementation of change management by maximizing the Project Management Office (PMO) function.

Risk Management System's Review on the Effectiveness

Throughout 2025, Telkom's risk management system has been operating effectively in managing various business risks to support every policy and process within the TelkomGroup. Telkom utilizes several risk management tools or information systems, including:

1. Generic Tools Enterprise Risk Management Online (ERM Online) which is used by all units for Risk Register management.
2. Specific Tools for specific risk management purposes e.g.:
    a. Fraud Management System (FRAMES) application is used for the early detection system of potential Customer and Third-Party Fraud.
    b. Telkom Legal Intelligence System (TELIS) is used as a repository for internal policy and external company regulation.
    c. ICoFR Control Self-Assessment (ICSA) is a tool or application used to facilitate the self-assessment process for the implementation of business process at the transaction level control (TLC) level and enable timely reporting of self-assessment result.
    d. EITA (Enterprise IT Architecture) application is an application that manages the ICoFR business process repository.

Telkom has also carried out an assessment process for the effectiveness of risk management implementation in 2025, namely:

1. Measurement of Risk Maturity Index (RMI).
2. Monitoring and evaluation of the effectiveness of risk mitigation through ERM Online application.
3. Evaluation/discussion and advisory on a one-on-one basis with business unit as needed.
4. Reporting and evaluation together with the BOD and Committee for Planning and Risk Evaluation and Monitoring (KEMPR).
5 Preparation and reporting document of 2025 Contingency Plan.

Statement of the Board of Directors and Board of Commissioners on Adequacy of Risk Management System

The Board of Directors and Board of Commissioners, through Committee for Planning and Risk Evaluation and Monitoring (KEMPR), regularly hold meetings with Risk Management Department to discuss risk monitoring throughout the company. This meeting also covers follow-up actions taken by risk owner to minimize identified risk. Risk Management Department reports the result of risk monitoring to the Board of Directors and Board of Commissioners on a quarterly basis, ensuring that risk management is carried out effectively and sustainably.