Telkom

Telkom SA SOC Ltd

Enterprise Risk Management Principles

For the year ended 31 March 2026

Seamlessly connecting
our customers to a better life

"The Group continues to enhance its risk management approach and framework. A full disclosure of Telkom's material risks are detailed herein, in compliance with the governance requirements contained in paragraph 8.63(s) of the JSE Listings Requirements."

Risk disclosure

(paragraph 8.63(s) of the JSE Listings Requirements)

The Telkom Group enterprise risk management policy is designed to uphold the Telkom Board's responsibility for enterprise risk and serves as a formal acknowledgment by both the Board and management of Telkom's dedication to the fundamental principles of risk management.

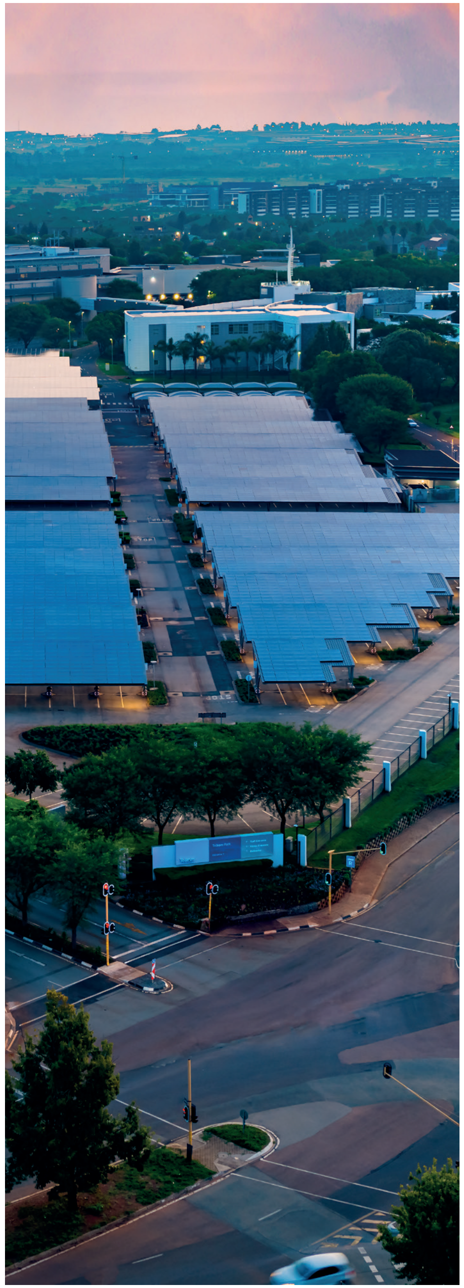
This policy provides guidance to executives and senior management, outlining the principles, requirements and responsibilities necessary for a robust approach to risk management and continuous internal control assurance. By adhering to these practices, Telkom aims to conduct business with integrity, promoting growth and sustainability amid the ever-changing economic, political, technological and social conditions within the business landscape in which the Group operates.

Telkom acknowledges enterprise risk management as a fundamental element of sound corporate governance. The Group is committed to the following principles:

- Instilling risk management into the organisation's culture and the way business is conducted across the entire Group
- Integrating enterprise risk management into strategy formulation, activity planning, performance management and resource allocation decisions
- Adhering to best practices in managing risks and capitalising on opportunities
- Analysing and assessing the Group's risk profile, aligning it with the risk appetite, and evaluating the effectiveness of risk responses and root causes in line with strategic objectives

Telkom ensures effective management of the Group's risks by:

- Recognising that robust risk management is crucial for sustainability and maintaining strong relationships with customers and other stakeholders in the long term
- Embedding risk and opportunity management consistently and coherently into Telkom's culture, in line with best practices
- Supporting the enterprise risk management strategy with capable individuals, efficient processes and appropriate technology, while upholding governance, risk and compliance requirements
- Acknowledging the interconnectedness of the Group's operations and fostering business resilience, including anticipating, monitoring and responding to both macro- and micro-environmental factors



Telkom's material and strategic risks, managed at the Group level, are outlined below in accordance with paragraph 8.63(s) of the JSE Listings Requirements. It is important to review these risk disclosures alongside Telkom Group's 2026 integrated report, which emphasises our materiality themes.

	Risk name	Risk definition	Mitigating and monitoring
1	Market forces and competition	The telecommunications industry continues to undergo structural disruption driven by over-the-top (OTT) providers, financial technology (fintech) companies, hyperscalers and mobile virtual network operators (MVNOs) entering the digital ecosystem. These players are eroding traditional voice and data revenue streams, intensifying price competition and reshaping customer expectations. In FY2026, pricing pressure, spectrum dynamics and convergence across industries increased the risk of margin compression and reduced differentiation. Telkom's long-term competitiveness depends on its ability to scale digital services, innovate rapidly and remain relevant in a highly dynamic and commoditising market.	- Strengthen market intelligence and competitive positioning - Expand fibre, pre-paid and digital services - Leverage strategic partnerships for growth - Enhance customer value propositions and retention
2	Cybersecurity and data protection	As Telkom expands its digital footprint and operates critical national infrastructure, it becomes a high-value target for increasingly sophisticated cyberthreats. These include ransomware, AI-enabled attacks and supply chain vulnerabilities. The external threat landscape continues to intensify, and a single breach can have systemic implications. Maintaining resilience, protecting customer data and ensuring uninterrupted service delivery are critical for sustaining trust and regulatory compliance.	- Enhance security operations and incident response capabilities - Implement zero-trust architecture and AI-driven monitoring - Strengthen third-party and ecosystem security controls - Drive organisation-wide cybersecurity awareness
3	Regulatory compliance	Telkom operates in a complex and evolving regulatory environment covering telecommunications, data privacy and digital services. Regulatory uncertainty and increasing compliance obligations elevate risk exposure. Failure to anticipate regulatory changes can constrain operations, increase costs and impact strategic execution.	- Strengthen regulatory and compliance frameworks and internal controls - Engage proactively with regulators - Continuously monitor legislative developments
4	Customer experience and brand	Customer expectations are increasingly shaped by digital-first experiences, reliability and responsiveness. Service failures, network issues and gaps in digital capability directly impact customer satisfaction, retention and brand perception. In a competitive market, customer experience is a key differentiator.	- Invest in network quality and digital platforms - Enhance customer experience programmes - Leverage analytics to improve retention
5	Workforce and skills	The pace of digital transformation is reshaping workforce requirements, with growing demand for skills in AI, cloud and advanced technologies. Telkom faces a structural gap between existing capabilities and future needs, increasing execution risk.	- Strengthen strategic workforce planning - Enhance upskilling and reskilling programmes - Advance leadership and talent development initiatives

	Risk name	Risk definition	Mitigating and monitoring
6	Sustainability	Environmental, social and governance (ESG) expectations continue to rise, with increasing focus on climate transition, governance and responsible business practices. ESG performance is directly linked to reputation, regulatory compliance and access to capital.	- Implement our 2030 Sustainability Strategy - Invest in energy efficiency - Strengthen ESG governance and reporting
7	Profitability and cash flow	Economic pressure, rising costs and pricing constraints impact profitability and cash generation. Maintaining financial resilience is critical for sustaining operations and funding growth.	- Optimise costs and improve efficiency programmes - Diversify revenue initiatives - Strengthened cash flow management
8	Network performance	Network reliability is central to Telkom's service delivery. Infrastructure challenges, outages and legacy systems create operational risks and impact customer experiences.	- Modernise and upgrade the network - Monitor and detect faults in real time - Invest in infrastructure resilience
9	Third-party risk	Increasing reliance on suppliers and partners introduces operational and security risks. Limited visibility into supplier ecosystems amplifies our risk exposure.	- Strengthen third-party risk frameworks - Enhance due diligence and monitoring - Implement supplier diversification strategies
10	Stakeholder management	Strong stakeholder relationships are important for regulatory alignment, investor confidence and strategic execution. Poor engagement can impact trust and reduce our influence.	- Engage and communicate proactively - Strengthen governance and transparency - Align with stakeholder expectations
11	Macro-economic conditions	Economic volatility affects customer demand, affordability and overall performance. Structural economic challenges continue to influence Telkom's growth prospects.	- Conduct scenario planning and monitoring - Implement cost management initiatives - Strengthen credit controls
12	Geopolitical risk	Global geopolitical instability impacts supply chains, costs and operational continuity. External shocks can have cascading business impacts.	- Diversify suppliers - Monitor geopolitical developments - Implement risk mitigation strategies