INTERNAL CONTROL SYSTEM

The Internal Control System (SPI) is a continuous monitoring mechanism that includes the reliability of financial reports and the availability of complete and timely financial reports, including the evaluation of financial reporting. SPI Telkom is run collectively by the Board of Directors, management, and other personnel under the supervision of the President Director and Director of Finance.

Through SPI, Telkom ensures that the preparation of consolidated financial reports is in accordance with the Financial Accounting Standards set by the Indonesian Institute of Accountants (IAI). Telkom's shares are listed on the New York Stock Exchange, therefore Telkom must also comply with the provisions of SOX Section 404, which requires Telkom to establish, maintain, test, and disclose the effectiveness of internal control over financial reporting.

SPI also ensures the achievement of efficiency and effectiveness of operational activities and compliance with regulations. Through SPI, Telkom can monitor the Company, compliance with applicable regulations, both regulations from Telkom officials and government regulations. Telkom can also control its operational activities in accordance with the work procedures in each function.

INTERNAL CONTROL FRAMEWORK

Telkom implements SPI in accordance with the Internal Control-Integrated Framework 2013 from The Committee of Sponsoring Organizations of the Treadway Commission (COSO). Telkom continues to ensure that all business activities are carried out in accordance with applicable laws and regulations. The Legal & Compliance Unit under the Corporate Secretary Department is responsible for statutory compliance, which carries out several activities, such as legal advisory, legal opinion, legal review, and litigation.

Telkom implements five internal control components with the COSO Framework, which are interconnected at all levels and business units of the Company,, namely.:

1. **Control Environment**
   a. Demonstrates commitment to integrity and ethical values.
   b. Exercises oversight responsibility.
   c. Establishes structure, authority, and responsibility.
   d. Demonstrates commitment to competence.
   e. Enforces accountability.

2. **Risk Assessment**
   a. Specifies relevant objectives.
   b. Identifies and analyzes risk.
   c. Assesses fraud risk.
   d. Identifies and analyzes significant change.

3. **Control Activities**
   a. Selects and develops control activities.
   b. Selects and develops general controls over technology.
   c. Deploys through policies and procedures.

4. **Information and Communication**
   a. Uses relevant information.
   b. Communicates internally.
   c. Communicates externally.

5. **Monitoring Activity**
   a. Conducts ongoing and/or separate evaluations.
   b. Evaluates and communicate deficiencies.

INTERNAL CONTROL IMPLEMENTATION IN TELKOM

Telkom implements and applies the COSO Framework components to its policies, namely:

Internal Control Implementation In Telkom

Control Environment
• Telkom is committed to integrity and ethical values by building and establishing a corporate culture as a guide for main players in building leadership patterns and strengthening organizational synergies, as an engine of economic growth, an accelerator of social welfare, a provider of employment, and a provider of high performing culture talent. Telkom guarantees sustainable competitive growth in the form of long-term superior performance achievement. Core Values AKHLAK (*Amanah, Kompeten, Harmonis, Loyal, Adaptif, and Kolaboratif*) are the main values of SOE human resources that must be adopted by TelkomGroup so that every TelkomGroup resource knows, implements, and internalizes seriously, consistently and consequently, thus bring forth to daily behaviors that shape the work culture of TelkomGroup which is in line with the Core Values of SOE. • Telkom ensures the effectiveness of implemented Internal Audit activities by implementing the SOA 302/404 prerequisites and managed with a risk-based audit approach. Telkom also ensures that effective coordination and co-operation with internal and external parties, and business risks to all business activities are adequately managed with internal control systems. • Telkom has a Competency Directory that defines the Telkom's competency needs. One of them is Finance Stream which includes the competence of Corporate Finance with the sub-area of capital structure competency and Working Capital Management (Treasury Management). Then, Accounting with sub-area competence of Financial Accounting, Management Accounting, and Corporate Tax. The competency development policy is aimed at creating superior, global quality, and highly competitive employees.
Risk Assessment
• Telkom has several considerations in developing accounting policies, such as Statements of Financial Accounting Standards (PSAK), Interpretation of Statements of Financial Accounting Standards (ISAK), International Accounting Standards (IAS), related laws, and changes in impacted internal environments. • Telkom has a principle of financial assertion in ICOFR planning that is well respected by all relevant employees. • Telkom manages internal and external corporate risk with established mechanisms. • Telkom also implements an anti fraud policy control system and has potential fraud prevention.
Control Activities
• Telkom sets up a Business Process Owner (BPO) and AO (Application Owner) that have duties and responsibilities related to ICOFR. • Risk determination rules and internal controls refer to the ICOFR policy consisting of segregation of duties, risk determination, and determination of internal controls. • Telkom has guidelines for the implementation of information systems security that are aligned with Telkom needs and can be implemented on an ongoing basis.
Information and Communication
• Telkom has accounting policies implemented under IFAS and IFRS, outlined following accounting principles and implementation, including information or data related to the process and disclosure of financial reporting, and regulates the components of the consolidated financial statements. • Telkom has an information technology policy that provides a frame of reference for each process or unit associated with the organization's IT operations in the preparation and implementation of guidelines and procedures. The scope of IT regulations in our Telkom covers aspects of IT governance and IT management.
Monitoring Activity
• Telkom has an Internal Audit Charter that includes the auditor's requirements in Internal Audit Department, which has professional integrity and behavior, knowledge of risks and important controls in the field of information technology, knowledge of Capital Market laws and regulations. • CEO TelkomGroup always increases awareness from management regarding audit and change management in the form of CEO Notes and establishes Integrated Audit and forms Probis IFRS.

In accordance with Minister of State-Owned Enterprises Regulation No. PER-01/MBU/2011 regarding the Implementation of Good Corporate Governance (GCG) in SOE, specifically Article 26 paragraph (2), Telkom carries out regular assessments of the implementation of SPI to improve the quality of SPI. The results of the SPI assessment in 2023 show that Telkom's Control System is effective.

FINANCIAL AND OPERATIONAL CONTROL

Financial control carried out by Telkom includes financial plans, feedback, adjustments, and validation processes to ensure plan implementation or change plans in response to various changes. Meanwhile, operational control consists of the deployment process to ensure operational activities run effectively and efficiently.

In general, financial and operational control at Telkom, includes:

1. **Physical Control of Assets and Intangible Assets**
   Physical control of assets in the corporate environment is directed at securing and protecting risky assets.
2. **Separation of Functions and Authorization**
   Segregation of functions is geared towards adequate review and reduces the potential for errors and fraud.
3. **Execution of Events and Transactions**
   Control is carried out to ensure that transaction activities are carried out properly according to the plan and need that have been determined.
4. **Accurate and On Time Records on Events and Transactions**
   Accurate and on time records of operational events and transactions that carried out.
5. **Restricted Access and Accountability for Resources and Their Records**
   Access to Telkom resources and records should be limited only to the personnel that assigned the duties and responsibilities.
6. **Good Documentation of Control Events and Transactions**
   Every event and transaction in the Company is well documented as basic evidence of the occurrence and fairness of the transaction.

EFFECTIVENESS OF INTERNAL CONTROL SYSTEM OVERVIEW

Telkom reviewed SPI's effectiveness based on supervision carried out by the Internal Audit (IA) and External Audit Departments. The IA Department submits SPI supervision reports to the Board of Directors and Board of Commissioners. Management is responsible for implementing an effective and reliable SPI and ensuring that this is embedded at every level of the Company.

The Internal Audit Department reports the results of SPI supervision to the Board of Directors and Board of Commissioners. The audit findings will be submitted to the relevant management for follow-up. Based on the supervision in 2023, Telkom's SPI is considered to have been running effectively.

STATEMENT OF THE BOARD OF DIRECTIONS AND/OR THE BOARD OF COMMISSIONERS ON ADEQUACY OF INTERNAL CONTROL SYSTEM

Through the Audit Committee, the Board of Directors and Board of Commissioners hold regular meetings with the Internal Audit and External Audit Departments to discuss internal control monitoring and follow-up plans on matters management needs to pay attention to. The Internal Audit and External Audit Unit reports the results of monitoring and testing of internal control to the Board of Directors and Board of Commissioners at least once a year.

The Board of Directors and Board of Commissioners assess that Telkom's internal control system has been running effectively and has met the adequacy of the policies and standards referred to, among others:

1. Provisions of Sarbanes-Oxley Act (SOX) 302, 404, and 906.
    a. **SOX 302 Corporate Responsibility for Financial Reports**
    Require the CEO and CFO to provide certification regarding the effectiveness of design and implementation of internal control and disclosure of significant deficiencies in internal control in the context of financial reporting (Internal Control over Financial Reporting/ICoFR).
    b. **SOX 404 Management Assessment of Internal Controls**
    Require companies that list their shares on United States stock exchange to design, implement, document, evaluate, and disclose the result of evaluation of the effectiveness of internal control over financial reporting (Internal Control over Financial Reporting/ICoFR).
    c. **SOX 906 Corporate Responsibilities for Financial Reports: Failure of Corporate Officers to Certify Financial Reports**
        i. If misrepresented, the CEO and CFO are subject to criminal penalties of up to $1 million or up to 10 years in prison, or both, or
        ii. If the disclosure is intentional, the CEO and CFO are subject to criminal penalties of up to $5 million or up to 20 years in prison, or both.
2. Regulation of Minister of State-Owned Enterprises Article 26 Paragraph 2 of 2011 regarding Implementation of Good Corporate Governance (GCG) in SOE.

RISK MANAGEMENT SYSTEM

The risk management system is essential in realizing Good Corporate Governance (GCG). By implementing a good risk management system within Telkom and its subsidiaries, the Company can identify various business risks faced and develop appropriate risk mitigation to expand the business scope for communication transformation in the digital era, improve the risk management system on an ongoing basis, and support business continuity.

GENERAL ILLUSTRATION REGARDING THE RISK MANAGEMENT SYSTEM

As a Company listed on the New York Stock Exchange (NYSE), Telkom is also required to implement risk management that complies with the Sarbanes-Oxley Act, significantly articles 302 and 404. Based on the Minister of State-Owned Enterprises Regulation No. PER-2/MBU/03/2023 regarding Guidelines for Governance and Significant Corporate Activities of State-Owned Enterprises, Telkom, as a state-owned Telkom, is also required to implement a risk management system. Implementing a risk management system is carried out to fulfill compliance aspects and maintain business continuity so that it runs well.

Telkom publishes various Telkom policies relating to risk management implementation arrangements, among others:

1. Decision of the Commissioners (KAKOM No. 7/2006 Risk Management regarding the Authorities and Responsibilities of the Commissioners, the Obligations of the Directors regarding the Implementation of Risk Management);
2. Resolution of the Board of Directors/Regulation of the Board of Directors (KD 13/2009regarding Guidelines for the Management of SOX Sections 302 and 404, Telkom Management refers to the provisions of the US SEC;
3. Regulation of the Board of Directors of a Limited Liability Telkom (Persero) (Number: 614.00/r/01/HK200/COP-D0030000/2021)regarding Telkom Risk Management;
4. Regulation of the Director of Finance and Risk Management (PR 614.00/r.01/HK200/COP-I0000000/2022regarding Guidelines for Implementing Corporate Risk Management (Telkom Enterprise Risk Management);
5. Standard Operation Procedure, (Number: SOP. RMPP.03/RSG/2022) regarding the explanation of the regulations for the director of finance and risk management for corporate companies (Persero) PR 614.00/r.01/HK200/COP-I0000000/2022 regarding implementation guidelines for enterprise risk management.

These various regulations and provisions form the foundation for Telkom to carry out risk management, of course referring to various existing standards and best practices.

RISK MANAGEMENT SYSTEM (FRAMEWORK) AND POLICY

Telkom's risk management implementation is based on two policies: Regulation of the Board of Directors No. PD.614.00/r.01/HK.200/COP-D0030000/2021 dated April 30, 2021 regarding Company Risk Management (Telkom Enterprise Risk Management) and Regulation of the Director of Finance and Risk Management No. PR.614.00/r.01/HK200/COP-I0000000/2022 regarding Guidelines for Implementing Enterprise Risk Management (Telkom Enterprise Risk Management). Since 2021, Telkom's risk management policy has referred to the ISO 31000:2018 Risk Management – Principles and Guidelines standard, which consists of 3 main components, namely:

1. Principle

Risk Management Principles as the foundation for how risk management works to ensure the creation and protection of value, including:

1) Integrated
   Risk management is an integrated part of the Company's overall activities.
2) Structured and Comprehensive
   In practice, the Company takes a structured and comprehensive approach to provide consistent and comparable results.
3) Costumized
   The risk management framework and process must be adapted and proportionate to the external and internal context of the organization in line with the Company's goals.

4) Inclusive
It is necessary to involve the right stakeholders at the right time to take their knowledge, views, and perceptions into account, thereby increasing awareness of risk management, which is well-informed.
5) Dynamic
Risks can appear, change, and disappear along with the changes in the context and conditions of the Company's internal and external environment. The application of risk management must be able to anticipate, detect, acknowledge, and respond to these changes and events in an appropriate and timely manner.
6) Best Available Information
Risk management is based on historical, current information, and expectations for the future. Risk management explicitly considers all limitations and uncertainties associated with such information and expectations. Information must be timely, clear, and available to relevant stakeholders.
7) Human and Culture Factors
Behavior and culture significantly affect all aspects of risk management at every level and stage of the Company's activities.
8) Continuous Improvement
Risk management is continuously improved through learning and experience.

2. Framework

The framework that regulates the commitment to the role and division of Telkom's risk management functions includes:

1) Leadership and Commitmen
   i. The Board of Directors ensures that risk management is integrated into all activities of the Company and must demonstrate leadership and commitment, by:
      a. Customize and implement all components of the framework;
      b. Issue a statement or policy that sets out risk management approaches, plans, or actions;
      c. Ensure that necessary resources are allocated to manage risk;
      d. Establish authority, responsibility, and accountability at the appropriate level within the Telkom.
   ii. Risk management becomes inseparable from the Company's objectives, governance, leadership and commitment, strategy, goals, and operations.
2) Integration
   i. Risk management becomes inseparable from the Telkom's objectives, governance, leadership and commitment, strategy, goals, and operations;
   ii. The integration of risk management into the Company is a dynamic and iterative process and must be adapted to the needs and culture of the Company.
   iii. Risks are managed in every part of the Companys structure, where everyone in the Company has the responsibility to manage risks.
3) Design
   i. The design of the risk management framework is carried out by examining and understanding the external and internal context of the Telkom.
   ii. The Board of Directors and the Board of Commissioners demonstrate and articulate their ongoing commitment to risk management through policies, statements, or other forms, and are communicated within the Company and stakeholders.
   iii. Authority, responsibility, and accountability related to risk management are established and communicated at all levels within the Company.
   iv. Management ensures the appropriate allocation of resources for risk management.
   v. The Company establishes approved communication and consulting approaches to support the framework and facilitate the implementation of effective risk management.
4) Implementation
Risk management implementation requires stakeholders' involvement and awareness, thus allowing the Company to consider uncertainty in decision-making explicitly.
5) Evaluation
The Company evaluates the effectiveness of the risk management framework by periodically measuring its performance of the risk management framework.

6) Improvement
   i. The Company monitors and adjusts the risk management framework in anticipation of external and internal changes.
   ii. The Company is constantly improving the suitability, adequacy, and effectiveness of the risk management framework and how to integrate risk management processes.

3. Context assignment - Scope, Context, and Criteria;

1) Risk assessment consisting of:
   i. Risk identification
      It is a process to find, recognize, and describe risks in achieving the Company's objectives. Relevant, appropriate, and up-to-date information is essential in identifying risks.
   ii. Risk Analysis
      It is a process to understand the nature and characteristics of risk, including its level of risk. Risk analysis involves a detailed consideration of the uncertainty, the source of the risk, the consequences, the possibilities, events, scenarios, controls, and their effectiveness. An event can have many causes and consequences and can also affect a variety of objectives.
   iii. Risk evaluation
      Is a process to support decision-making. Risk evaluation involves comparing risk analysis results with established risk criteria to determine where additional measures are needed.
2) Risk treatment
   i. Risk treatment is to select and implement options for dealing with risk, which consists of:
      a. Risk aversion
      b. Accept risk
      c. Mitigating risk
      d. Dividing/transferring risk
   ii. The risk treatment plan should be integrated into the Company's management plans and processes in consultation with appropriate stakeholders.
3) Monitoring dan review
   i. Monitoring and review are to ensure and improve the quality and effectiveness of the process design, implementation, and risk management outcomes.
   ii. Monitoring and review should be carried out at all process stages, including planning, collecting, analyzing information, documenting results, and providing feedback.
4) Recording and Reporting
   i. The risk management process and its results should be documented and reported through appropriate mechanisms.
   ii. Reporting is an integral part of corporate governance. It is intended to improve the quality of dialogue with stakeholders and support the Board of Directors and the Board of Commissioners in fulfilling their responsibilities.