Internal Control System

Internal Control System (SPI) is a continuous monitoring mechanism implemented to ensure the reliability and timeliness of Financial Statements, as well as to evaluate such reporting. Telkom's SPI is implemented collectively by the Board of Directors, management, and relevant personnel, under the supervision of the President Director and the Director of Finance and Risk Management.

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). As a company whose shares are listed on New York Stock Exchange, Telkom is also required to comply with Sarbanes-Oxley Act (SOX) Section 404, which requires companies to establish, maintain, test, and report on the effectiveness of internal controls over financial reporting.

SPI also plays a crucial role in ensuring operational efficiency and effectiveness, as well as ensuring compliance with applicable regulations. Through SPI, Telkom can monitor compliance with internal policies and government regulations, while controlling operational activities in accordance with work procedures established in each organizational function.

Internal Control Framework

Telkom implements an Internal Control System (SPI) in accordance with 2013 Internal Control-Integrated Framework issued by Committee of Sponsoring Organizations of the Treadway Commission (COSO). Telkom ensures that all its business activities comply with applicable laws and regulations. Responsibility for legal compliance rests with the Legal & Compliance Unit, which is under the Corporate Secretary Department. This unit carries out various activities, such as providing legal advisory, legal opinion, legal review, and handling 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 suitable 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	
1.	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.
2.	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 system.
3.	Telkom has a Competency Directory that defines the company's competency needs. One of them is Stream Finance which includes competence of Corporate Finance with the sub area competence of Capital Structure 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	
4.	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.
5.	Internal Control over Financial Reporting (ICoFR) is designed on the principle of risk-based assessment.
6.	Telkom has a principle of financial assertion in ICoFR planning that is well respected by all relevant employees.
7.	Telkom manages internal and external corporate risk with established mechanisms.
8.	Telkom also implements an anti-fraud policy control system and has potential fraud prevention.
Control Activities	
9.	The governance of ICoFR control activities in Telkom applies the three-line model, where the business unit (Business Process Owner) is responsible for control implementation as the first line, Risk Management as the second line for ensuring the suitability of control design, and Internal Audit as the third line for assessing the effectiveness of control design compared to operational implementation.
10.	Telkom establishes and updates the ICoFR design, which consists of Entity-Level Control (ELC), Transactional-Level Control (TLC), and IT General Control (ITGC), regularly.
11.	Telkom sets up a Business Process Owner (BPO) and AO (Application Owner) that have duties and responsibilities related to ICoFR.
12.	Risk determination rules and internal controls refer to the ICoFR policy consisting of segregation of duties, risk determination, and determination of internal controls.
13.	Telkom has guidelines for the implementation of information system security that are aligned with company needs and can be implemented on an ongoing basis.
14.	Telkom conducts ICoFR Control Self-Assessment (CSA) to assess the design's effectiveness periodically.

Information and Communication	
15.	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.
16.	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 company covers aspects of IT governance and IT management.
Monitoring Activity	
17.	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.
18.	CEO TelkomGroup always increases awareness from management regarding audit and change management in the form of CEO Notes and establishes Integrated Audit.

In accordance with Regulation of Minister of State-Owned Enterprises No. PER-2/MBU03/2023 regarding Guidelines for Governance and Significant Corporate Activities in State-Owned Enterprises, Telkom routinely assesses the implementation of Internal Control Systems (SPI) to improve its quality. The 2025 SPI assessment results indicate that Telkom's Control System is effective.

Financial and Operational Control

Telkom's financial control covers financial planning, feedback, adjustment, and validation processes to ensure the implementation of plans or to change plans in response to changes that occur. Meanwhile, operational control covers monitoring and regulation processes to ensure that operational activities are carried out 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**

   Separation 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 needs 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 are carried out.

5. **Restricted Access and Accountability for Resources and Their Records**

   Access to company 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 is responsible for submitting SPI supervision report to the Board of Directors and Board of Commissioners. Management is responsible for ensuring that effective and reliable SPI are implemented throughout the organization.

Any monitoring findings by Internal Audit Department are reported to the Board of Directors and the Board of Commissioners, who then forward these findings to relevant management for follow-up. Based on the monitoring conducted throughout 2025, Telkom's Internal Audit Unit was deemed to have functioned effectively.

Statement of the Board of Directions and/or the Board of Commissioners on Adequacy of Internal Control System

The Board of Directors and Board of Commissioners, through the Audit Committee, regularly hold meetings with the Internal Audit Department and External Audit to discuss internal control monitoring and follow-up plans for issues that require management's attention. During these meetings, the results of internal control monitoring and follow-up measures to be taken are discussed. The IA and External Audit Department report the results of internal control monitoring and testing 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 SPI has been running effectively and meets the requirements of the policies and standards referred to, including:

1. **Provisions of 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 the 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 the Minister of SOE No.PER-2/MBU03/2023 regarding Guidelines for Governance and Significant Corporate Activities at State-Owned Enterprises**