Tata Kelola Teknologi Informasi
Information Technology Governance

Perusahaan secara berkelanjutan memperkuat pemanfaatan Teknologi Informasi (TI) sebagai bagian dari transformasi bisnis dan penguatan tata kelola perusahaan. Pengembangan teknologi diarahkan untuk mendukung efektivitas operasional dan peningkatan kinerja, seraya menciptakan proses kerja yang lebih transparan, terintegrasi, dan responsif terhadap kebutuhan bisnis. Pemanfaatan TI ini turut mendukung penerapan prinsip-prinsip governansi korporat, sehingga tercipta tata kelola yang semakin akuntabel, efisien, dan adaptif terhadap dinamika industri.

LANDASAN KEBIJAKAN DAN KERANGKA TATA KELOLA TI

Proses governansi atas risiko TI dijalankan secara terintegrasi melalui tiga landasan kebijakan Direksi yang saling melengkapi, yaitu Peraturan Direksi Nomor PER.0004/HK.01.06/PLMT-2021 tentang Pedoman Tata Kelola Bidang Teknologi Informasi (mencakup Pedoman Information Technology Governance dan Pedoman Tata Kelola Data), serta Peraturan Direksi Nomor PU.05.02/7/11/2/RINO/DIRU/PLMT-23 tanggal 7 November 2023 tentang Pedoman Business Continuity Management (BCM) yang mengacu pada standar internasional best practice ISO 22301:2019. Ketiga kebijakan ini memastikan risiko gangguan sistem (disruption), keamanan siber (cyber security), dan pemulihan bencana (disaster recovery) dikelola melalui satu siklus tata kelola yang utuh dan berlapis: identifikasi, analisis, mitigasi, pengujian, eskalasi, hingga pelaporan kepada Direksi.

ROADMAP TEKNOLOGI INFORMASI PERUSAHAAN

Pengembangan Teknologi Informasi (TI) di lingkungan Perusahaan dilakukan secara terarah dan selaras dengan agenda transformasi bisnis jangka panjang, yang mengacu pada Rencana Jangka Panjang Perusahaan (RJPP) periode 2021–2025 serta *roadmap* pengembangan TI Pelindo sebagai *Holding* BUMN Kepelabuhanan untuk periode 2022–2026.

Transformasi digital tersebut kemudian diterjemahkan ke dalam tema pengembangan 5 (lima) tahunan yang menjadi panduan implementasi berbagai inisiatif TI di lingkungan Perusahaan. Adapun gambaran transformasi digital dimaksud adalah sebagai berikut:

The Company continuously strengthens the use of Information Technology (IT) as part of its business transformation and strengthening corporate governance. Technology development is aimed at supporting operational effectiveness and improving performance, while creating more transparent, integrated, and responsive work processes to business needs. This IT utilization also supports the implementation of corporate governance principles, resulting in increasingly accountable, efficient, and adaptive governance that adapts to industry dynamics.

IT POLICY FOUNDATIONS AND GOVERNANCE FRAMEWORK

The IT risk governance process is carried out in an integrated manner through three complementary Board of Directors policy foundations, namely Board of Directors Regulation No. PER.0004/HK.01.06/PLMT-2021 concerning Guidelines for Information Technology Governance (covering the Information Technology Governance Guidelines and Data Governance Guidelines), as well as Board of Directors Regulation No. PU. 05.02/7/11/2/RINO/DIRU/PLMT-23 dated November 7, 2023, on Business Continuity Management (BCM) Guidelines, which reference the international best practice standard ISO 22301:2019. These three policies ensure that risks related to system disruption, cybersecurity, and disaster recovery are managed through a comprehensive, multi-layered governance cycle: identification, analysis, mitigation, testing, escalation, and reporting to the Board of Directors.

CORPORATE INFORMATION TECHNOLOGY ROADMAP

Information Technology (IT) development within the Company is carried out in a targeted manner and aligned with the long-term business transformation agenda, which refers to the Company's Long-Term Plan (RJPP) for the 2021–2025 period and Pelindo's IT development roadmap as a State-Owned Port Holding Company for the 2022–2026 period.

This digital transformation is then translated into five-year development themes that serve as guidelines for the implementation of various IT initiatives within the Company. The following is an overview of the digital transformation:

2022 *Business Transition and Restructurization*	2023 *Digital Transformation Foundation*	2024 *System Enhancement*	2025 *Business Optimization*	2026 *Advancing Business Sustainability*
ITMP PMT diawali dengan restrukturisasi organisasi Pelindo Group di mana terjadi merger, serah terima operasi bisnis yang pada akhirnya mendorong seluruh entitas di Pelindo Group untuk membuat pedoman dan perencanaan pengembangan TI (*digital transformation*) ITMP PMT begins with the implementation of Pelindo Group's organizational restructuring where there is a merger, handover of asset operations and handover of business operations which ultimately encourages all entities in Pelindo Group to make IT development guidelines & planning (digital transformation)	Pada tahun 2023, tema ITMP berfokus pada penguatan fondasi organisasi perusahaan serta pengingkatan budaya digital sehingga perusahaan dapat lebih siap mendorong transformasi di lingkungan PMT. In 2023, ITMP theme focuses on strengthening the Company's organizational foundation and improving digital culture so that the Company can be better prepared to drive transformation in PMT environment.	Memasuki tahun 2024 terjadi peningkatan kolaborasi dan strategi bisnis di lingkungan PMT serta Pelindo Group yang didukung oleh penguatan sistem dan teknologi yang digunakan. Penerapan sistem dan teknologi yang semakin modern akan membantu organisasi perusahaan agar semakin terbiasa dengan budaya digital. Entering 2024 there is an increase in collaboration and business strategies within PMT and Pelindo Group supported by strengthening the systems and technology used. The application of increasingly modern systems and technology will help Company organizations to become more accustomed to digital culture.	**Tema ITMP di tahun ini berfokus pada upaya optimalisasi nilai atau manfaat yang didapat melalui investasi terhadap inisiatif ITMP.** This year's ITMP theme focuses on efforts to optimize the value or benefits gained through investment in each ITMP initiative.	Sedangkan di tahun terakhir ini, tema ITMP berfokus untuk meningkatkan keberlanjutan bisnis perusahaan melalui *continuous improvement* atas masing-masing inisiatif, baik dari segi bisnis, infrastruktur TI, keamanan TI, maupun organisasi TI. While in this final year, the ITMP theme focuses on improving the Company's business sustainability through continuous improvement of each initiative, both in terms of business, IT infrastructure, IT stability and IT organization.

REALISASI PROGRAM KERJA TI TAHUN 2025

Sepanjang tahun 2025, pengembangan dan implementasi teknologi informasi difokuskan untuk pengamanan pendapatan dalam penyesuaian sistem-sistem pada *Branch* yang dilakukan Transformasi Digitalisasi, Serah Operasi serta *Switching Invoice* PTP. Adapun realisasi pengembangan dan implementasi teknologi informasi hingga akhir tahun 2025 meliputi hal-hal sebagai berikut:

1. Transformasi dan Digitalisasi: *Branch* Jamrud, Tj Wangi, Tj Intan, Bagendang, Bumiharjo, Makassar, Balikpapan, Dumai, Belawan, Trisakti, Lembar, Gilimas, Tj Emas, Gresik, Pare-pare, Tj. Balai Karimun;
2. *Switching Invoice*: *Branch* Tj. Pandan, Teluk Bayur, Tj. Priok, Jambi dan Pangkal Balam, *Branch* Panjang, Palembang, Kijing dan Banten;
3. Transformasi dan Digitalisasi Terminal di Lingkungan PT Pelabuhan Tanjung Priok.

Implementasi Aplikasi

1. Aplikasi *Back End*:
   a. Single ERP SAP telah diimplementasikan pada tanggal 1 Oktober 2024 di PT Pelindo Multi Terminal sebagai dukungan untuk pencatatan keuangan yang lebih efisien dan terintegrasi, guna meningkatkan transparansi, akurasi, serta kecepatan dalam proses pengelolaan data keuangan dan operasional. Implementasi ini juga bertujuan untuk mendukung transformasi digital perusahaan dalam mencapai tujuan bisnis jangka panjang;

REALIZATION OF THE 2025 INFORMATION TECHNOLOGY WORK PROGRAM

Throughout 2025, the development and implementation of information technology were focused on revenue assurance through system adjustments at branches undergoing Digital Transformation, Operational Handover, and PTP Invoice Switching. As of the end of 2025, the realization of information technology development and implementation included the following:

1. Transformation and Digitalization: Jamrud, Tanjung Wangi, Tanjung Intan, Bagendang, Bumiharjo, Makassar, Balikpapan, Dumai, Belawan, Trisakti, Lembar, Gilimas, Tanjung Emas, Gresik, Parepare, and Tanjung Balai Karimun Branches;
2. Invoice Switching: Tanjung Pandan, Teluk Bayur, Tanjung Priok, Jambi, Pangkal Balam, Panjang, Palembang, Kijing, and Banten Branches;
3. Transformation and Digitalization of Terminals within PT Pelabuhan Tanjung Priok.

Application Implementation

1. Back-End Applications:
   a. a. Single ERP SAP was implemented on 1 October 2024 at PT Pelindo Multi Terminal to support more efficient and integrated financial recording, thereby enhancing transparency, accuracy, and timeliness in the management of financial and operational data. This implementation also supports the Company's digital transformation in achieving its long-term business objectives;

b. Implementasi Aplikasi Surat Menyurat (PEO) sebagai aplikasi surat menyurat, pembuatan Berita Acara pada PT Pelindo Multi Terminal;
c. Implementasi aplikasi Absensi (My Intan) sebagai aplikasi absensi yang akan digunakan di wilayah kerja PT Pelindo Multi Terminal;
d. Implementasi aplikasi perjalanan dinas (My Travel) sebagai aplikasi perjalanan dinas yang akan digunakan di wilayah kerja PT Pelindo Multi Terminal;
e. Implementasi aplikasi kantin (My Canteen) sebagai aplikasi untuk mempermudah proses permakanan pekerja dengan pengelolaan *voucher* saldo dan akses untuk pembelian berbagai macam makanan dan minuman yang akan digunakan di wilayah kerja PT Pelindo Multi Terminal;
f. Implementasi Modul *Material Management* (MM) Centra sebagai aplikasi pengadaan di Lingkungan PT Pelindo Multi Terminal;
g. Implementasi Aplikasi Prima (Pelindo Risk Management) sebagai system yang digunakan untuk memfasilitasi pengelolaan risiko operasional perusahaan;
h. Implementasi Aplikasi *Single Procurement System* (*Secure*) sebagai *system* yang digunakan untuk pelaksanaan lelang/tender secara *online*;
i. Implementasi Aplikasi Portaverse sebagai system yang digunakan untuk mengelola hal-hal terkait dengan *performance management system, training management system, learning management system*, dan *knowledge management system*;
j. Implementasi Aplikasi Cistle sebagai sebagai sistem yang digunakan untuk melakukan konsolidasi transaksi *intercompany* di PMT Group.

2. Aplikasi *Front End*:
   a. Pembuatan *Corporate Website* sebagai wadah informasi kepada pengguna jasa PT Pelindo Multi Terminal untuk mendapatkan informasi tentang PT Pelindo Multi Terminal;
   b. Implementasi Aplikasi GenC dan PTOS M sebagai aplikasi *Front End* pada Cabang PT Pelindo Multi Terminal yang terintegrasi dengan SAP dan aplikasi lainnya;
   c. Implementasi Aplikasi Spinner untuk mendukung adanya layanan baru petikemas;
   d. Penerapan Sistem *Gate* Timbangan;
   e. Implementasi Aplikasi PTOS PK (petikemas) sebagai aplikasi *Front End* pada Cabang PT Pelindo Multi Terminal yang terintegrasi dengan SAP dan aplikasi lainnya.

Penerapan Sistem Gate Timbangan

1. Pembuatan *Dashboard* Fasilitas sebagai *dashboard* manajemen untuk Bidang Fasilitas;
2. Pemeliharaan *Corporate Email* sebagai *email* PT Pelindo Multi Terminal;
3. *Office Supply* terkait Perangkat Teknologi Informasi untuk perangkat kerja untuk pegawai yang ditempatkan di PMT dalam mendukung pekerjaannya.

b. Implementation of the Correspondence Application (PEO) as the official correspondence and Minutes of Meeting application at PT Pelindo Multi Terminal;
c. Implementation of the Attendance Application (My Intan) as the attendance system to be used across PT Pelindo Multi Terminal's operational areas;
d. Implementation of the Business Travel Application (My Travel) as the official business travel application to be used across PT Pelindo Multi Terminal's operational areas;
e. Implementation of the Canteen Application (My Canteen) to facilitate employee meal services through voucher balance management and access for purchasing various food and beverages across PT Pelindo Multi Terminal's operational areas;
f. Implementation of the Material Management (MM) Centra Module as the procurement application within PT Pelindo Multi Terminal;
g. Implementation of the PRiMa (Pelindo Risk Management) Application as the system used to facilitate the management of the Company's operational risks;
h. Implementation of the Single Procurement System (Secure) as the system used to conduct online procurement and tender processes;
i. Implementation of the Portaverse Application as the system used to manage the performance management system, training management system, learning management system, and knowledge management system;
j. Implementation of the Cistle Application as the system used to consolidate intercompany transactions within the PMT Group.

2. Front-End Applications:
   a. Development of the Corporate Website as an information portal for PT Pelindo Multi Terminal's service users to obtain information about the Company;
   b. Implementation of the GenC and PTOS M Applications as front-end applications at PT Pelindo Multi Terminal branches, integrated with SAP and other applications;
   c. Implementation of the Spinner Application to support the new container service;
   d. Implementation of the Weighbridge Gate System;
   e. Implementation of the PTOS PK (Container) Application as a front-end application at PT Pelindo Multi Terminal branches, integrated with SAP and other applications.

Implementation of the Weighbridge Gate System

1. Development of the Facilities Dashboard as a management dashboard for the Facilities Division;
2. Maintenance of the Corporate Email System for PT Pelindo Multi Terminal;
3. Provision of Office Supplies related to Information Technology Equipment to support employees assigned to PMT in carrying out their duties.

Tata Kelola

1. Peraturan Direksi tentang Pedoman Tata Kelola Bidang TI sebagai dasar pelaksanaan Tata Kelola di lingkungan PT Pelindo Multi Terminal;
2. Keputusan Direksi tentang Information Technology Steering Commite untuk mempercepat proses perencanaan dan pengembangan Teknologi Informasi di lingkungan PT Pelindo Multi Terminal;
3. Dokumen Standar Prosedur Operasi (SPO) Divisi Teknologi Informasi.

PENGENDALIAN KETAHANAN DAN KEAMANAN SIBER

Perusahaan terus memperkuat pengelolaan dan pengembangan sistem Teknologi Informasi (TI) dengan menempatkan keamanan informasi sebagai salah satu prioritas utama. Penerapan sistem keamanan dilakukan untuk menjaga kerahasiaan data (*confidentiality*), keutuhan informasi (*integrity*), ketersediaan sistem (*availability*), serta kesiapan pemulihan ketika terjadi gangguan atau kondisi darurat (*disaster recovery*).

IDENTIFIKASI DAN MANAJEMEN RISIKO TEKNOLOGI INFORMASI

Identifikasi dan pengelolaan risiko TI dilaksanakan melalui proses manajemen risiko yang terstruktur dalam tujuh tahap, meliputi penetapan konteks, identifikasi risiko, analisis risiko, evaluasi risiko, penanganan risiko, komunikasi dan konsultasi, serta pemantauan risiko secara berkelanjutan. Proses ini dijalankan oleh Departemen Pengendalian Sistem, dengan penetapan tingkat risiko menggunakan matriks risiko berbasis kombinasi kemungkinan (probabilitas) dan dampak (severitas), serta opsi penanganan risiko yang mencakup *accept*, *avoid*, *control/mitigate*, dan *transfer*. Manajemen memastikan adanya kesadaran risiko (*risk awareness*) secara eksplisit pada tingkat pejabat eksekutif dan Direksi, sehingga akuntabilitas atas risiko TI yang signifikan tidak berhenti pada level teknis, melainkan menjadi bagian dari kesadaran manajemen puncak.

Sebagai mekanisme pengujian independen atas efektivitas pengendalian TI, Perusahaan melaksanakan audit TI secara berkala minimal satu kali dalam setahun, dilakukan oleh Satuan Pengawas Intern dan/atau auditor eksternal yang independen dan kompeten. Resume hasil audit TI dilaporkan kepada manajemen dan disosialisasikan oleh Senior Vice President Teknologi Informasi, dengan tindak lanjut korektif dan preventif yang dimonitor oleh Departemen Pengendalian Sistem melalui Laporan Monitoring Rekomendasi hingga tuntas sebelum tanggal target penyelesaian. Laporan-laporan strategis terkait TI, termasuk hasil audit dan rencana penggunaan TI, disetujui secara berjenjang oleh Senior Vice President Teknologi Informasi serta Direksi, memastikan risiko dan kinerja pengendalian TI senantiasa berada dalam pengawasan manajemen puncak.

Governance

1. Board of Directors' Regulation on Information Technology Governance Guidelines as the basis for IT governance implementation within PT Pelindo Multi Terminal;
2. Board of Directors' Decree on the Information Technology Steering Committee to accelerate the planning and development of Information Technology within PT Pelindo Multi Terminal;
3. Standard Operating Procedure (SOP) Documents of the Information Technology Division.

CYBER RESILIENCE AND SECURITY MANAGEMENT

The Company continues to strengthen the management and development of its Information Technology (IT) systems by placing information security as one of its key priorities. Security measures are implemented to safeguard data confidentiality, information integrity, system availability, and disaster recovery readiness in the event of disruptions or emergency situations.

IDENTIFICATION AND MANAGEMENT OF INFORMATION TECHNOLOGY RISK

Identification and management of IT risk is carried out through a structured risk management process comprising seven stages: context establishment, risk identification, risk analysis, risk evaluation, risk treatment, communication and consultation, and continuous risk monitoring. This process is carried out by the System Control Department, with risk levels determined using a risk matrix based on a combination of likelihood (probability) and impact (severity), and risk treatment options including accept, avoid, control/mitigate, and transfer. Management ensures explicit risk awareness at the executive and Board of Directors level, so that accountability for significant IT risks does not stop at the technical level but becomes part of top management's awareness.

As an independent testing mechanism for the effectiveness of IT controls, the Company conducts IT audits periodically at least once a year, carried out by the Internal Audit Unit and/or independent and competent external auditors. A summary of the IT audit results is reported to management and communicated by the Senior Vice President of Information Technology, with corrective and preventive follow-up actions monitored by the System Control Department through a Recommendation Monitoring Report until completion prior to the target resolution date. Strategic IT-related reports, including audit results and IT utilization plans, are approved in a tiered manner by the Senior Vice President of Information Technology and the Board of Directors, ensuring that IT risk and control performance remain under the continuous oversight of top management.

KEAMANAN SIBER DAN SISTEM MANAJEMEN PENGAMANAN INFORMASI

Pada aspek keamanan informasi, Direksi menunjukkan kepemimpinan dan komitmen secara eksplisit melalui penerapan Sistem Manajemen Pengamanan Informasi (SMPI), antara lain dengan memastikan keselarasan tujuan dan kebijakan pengamanan informasi dengan arahan strategis Perusahaan, serta ketersediaan sumber daya yang memadai. Manajemen Risiko Pengamanan Informasi (MRPI) diselenggarakan secara terintegrasi dan selaras dengan proses Enterprise Risk Management (ERM) Perusahaan, dengan asesmen risiko pengamanan informasi yang dilakukan secara rutin setiap enam bulan atau lebih cepat apabila terdapat perubahan proses bisnis yang berdampak signifikan terhadap profil risiko. Hasil asesmen dituangkan dalam Risk Treatment Plan (RTP) Keamanan Informasi yang disosialisasikan kepada stakeholder terkait untuk membangun kesadaran, keterlibatan, dan kepemilikan atas risiko keamanan informasi di seluruh lini organisasi.

Pada level operasional, penanganan insiden TI — termasuk insiden yang dikategorikan sebagai insiden keamanan siber — mengikuti jalur eskalasi berjenjang: penanganan awal oleh Departemen Pemeliharaan Sistem dan Data Manajemen sebagai *first level*, eskalasi kepada *Second Layer Support* apabila tidak dapat diselesaikan, hingga eskalasi kepada Vice President Pemeliharaan Sistem dan Manajemen Data untuk insiden yang dikategorikan sebagai insiden pengamanan informasi. Dengan mekanisme ini, setiap indikasi ancaman siber dapat ditangani secara terstruktur sekaligus diukur tingkat keparahannya sebelum ditentukan perlu tidaknya eskalasi lebih lanjut ke prosedur kontinuitas bisnis.

BUSINESS CONTINUITY MANAGEMENT (BCM) DAN DISASTER RECOVERY PLAN (DRP)

Kesiapan pemulihan bencana dikelola melalui mekanisme kontinuitas TI yang secara eksplisit melibatkan Direksi: Direksi menetapkan tim penyusun kontinuitas TI untuk menyusun *Disaster Recovery Plan* (DRP), yang didasarkan pada *Business Impact Analysis* (BIA) untuk menetapkan *Recovery Time Objective*/RTO dan *Recovery Point Objective*/RPO, serta *Risk Assessment* untuk menentukan strategi dan arsitektur kontinuitas yang memadai. Direksi selanjutnya melakukan reviu dan menetapkan kebijakan DRP sebagai referensi pengendalian risiko bencana, sementara pengujian DRP dilaksanakan secara berkala minimal satu kali dalam setahun untuk memastikan kecukupan rencana pemulihan sekaligus menghasilkan *lesson learned* bagi penyempurnaan berkelanjutan.

Secara kelembagaan, kesiapan menghadapi gangguan atau bencana diatur melalui struktur *Business Continuity Management* (BCM) yang terdiri dari empat tingkatan (BCM Level), disesuaikan dengan tingkat dampak gangguan terhadap layanan dan reputasi Perusahaan. Insiden yang dikategorikan sebagai kejadian luar biasa atau *disaster* akan dieskalasi langsung ke prosedur DRP, dan penanganan gangguan TI secara teknis dijalankan oleh

CYBERSECURITY AND THE INFORMATION SECURITY MANAGEMENT SYSTEM

In the area of information security, the Board of Directors demonstrates explicit leadership and commitment through the implementation of the Information Security Management System (ISMS), including by ensuring alignment of information security objectives and policies with the Company's strategic direction, as well as the availability of adequate resources. Information Security Risk Management (ISRM) is conducted in an integrated manner and aligned with the Company's Enterprise Risk Management (ERM) process, with information security risk assessments carried out regularly every six months, or more frequently in the event of business process changes that significantly affect the risk profile. The assessment results are set out in an Information Security Risk Treatment Plan (RTP), which is communicated to relevant stakeholders to build awareness, engagement, and ownership of information security risk across all levels of the organization.

At the operational level, IT incident handling — including incidents categorized as cybersecurity incidents — follows a tiered escalation path: initial handling by the System Maintenance and Data Management Department as the first level, escalation to Second Layer Support if unresolved, and further escalation to the Vice President of System Maintenance and Data Management for incidents categorized as information security incidents. Through this mechanism, any indication of a cyber threat can be handled in a structured manner while its severity is assessed to determine whether further escalation to the business continuity procedure is required.

BUSINESS CONTINUITY MANAGEMENT (BCM) AND DISASTER RECOVERY PLAN (DRP)

Disaster recovery readiness is managed through an IT continuity mechanism that explicitly involves the Board of Directors: the Board of Directors appoints the IT continuity planning team to develop the Disaster Recovery Plan (DRP), which is based on a Business Impact Analysis (BIA) to determine the Recovery Time Objective (RTO) and Recovery Point Objective (RPO), as well as a Risk Assessment to determine an adequate continuity strategy and architecture. The Board of Directors subsequently reviews and establishes the DRP policy as a reference for disaster risk control, while DRP testing is conducted periodically at least once a year to ensure the adequacy of the recovery plan and to generate lessons learned for continuous improvement.

Institutionally, readiness to face disruptions or disasters is governed through a Business Continuity Management (BCM) structure consisting of four levels (BCM Levels), calibrated to the level of impact of the disruption on the Company's services and reputation. Incidents categorized as extraordinary events or disasters are escalated directly to the DRP procedure, and technical handling of IT disruptions is carried out by

Tim Pemulihan IT dalam struktur Tim Penanganan Gangguan BCM, yang bertanggung jawab melakukan *damage assessment*, memastikan DRP berjalan efektif, serta menyatakan kesiapan sistem untuk kembali beroperasi normal.

PROSES IDENTIFIKASI HINGGA ESKALASI DAN PELAPORAN KEPADA DIREKSI

Untuk memastikan risiko TI yang teridentifikasi dikelola dan dilaporkan secara berjenjang kepada Direksi, setiap gangguan dideklarasikan sesuai tingkatan BCM Level oleh pejabat yang berwenang: Branch Manager untuk BCM Level 4, *Senior Vice President* terkait untuk BCM Level 3, Direktur Teknis untuk BCM Level 2, hingga gangguan pada tingkat tertinggi (BCM Level 1), yaitu yang berdampak pada reputasi Perusahaan, yang dideklarasikan dan ditetapkan langsung oleh Direktur Utama. Struktur ini memastikan bahwa semakin besar dampak suatu gangguan, semakin tinggi pula tingkat pejabat yang terlibat dalam pengambilan keputusan, dengan Direksi menjadi titik akhir eskalasi untuk risiko yang paling signifikan.

Keterhubungan antara fungsi teknis TI dengan Direksi turut diperkuat melalui Komite Pengarah TI (*IT Steering Committee*), yang berperan memberikan rekomendasi kepada Direksi atas Master Plan TI serta melakukan verifikasi sebelum Direksi menetapkannya, sekaligus menjadi pihak yang menyetujui perubahan-perubahan besar (mayor) atas sistem dan infrastruktur TI Perusahaan. Melalui rangkaian mekanisme ini, manajemen risiko tujuh tahap, audit TI tahunan, asesmen risiko keamanan informasi semesteran, pengujian DRP tahunan, eskalasi BCM berjenjang hingga Direktur Utama, dan pengawasan Komite Pengarah TI, Perusahaan memastikan bahwa risiko utama TI, baik yang bersifat operasional, keamanan siber, maupun bencana, senantiasa terverifikasi secara berkala dan bukan sekadar kebijakan yang statis.

PENELITIAN DAN PENGEMBANGAN

Perusahaan saat ini tengah memperkuat koordinasi dengan PT Pelabuhan Indonesia (Persero) dalam mendukung pengembangan kawasan strategis nasional di Kawasan Industri Terpadu Batang (KITB). Dalam proyek tersebut, Perusahaan diproyeksikan berperan sebagai operator terminal multipurpose nonpetikemas yang akan mendukung aktivitas logistik dan distribusi di kawasan industri dimaksud.

Sebagai subholding yang berfokus pada layanan terminal multipurpose, Perusahaan menyiapkan dukungan operasional melalui pengembangan suprastruktur serta sistem teknologi informasi yang dirancang untuk menunjang kelancaran aktivitas bongkar muat dan operasional pelabuhan secara terintegrasi.

Terminal tersebut diperkirakan akan melayani berbagai jenis muatan strategis, antara lain pasir silika untuk kebutuhan industri kaca, material baja, serta gas. Saat ini, Perusahaan masih melakukan kajian internal terkait potensi bisnis dan kebutuhan operasional, sekaligus menjalin komunikasi dan penjajakan dengan calon pengguna jasa sebagai bagian dari persiapan pengembangan layanan di kawasan tersebut.

the IT Recovery Team within the BCM Disruption Handling Team structure, which is responsible for conducting damage assessments, ensuring the DRP is effectively implemented, and confirming system readiness to resume normal operations.

PROCESS FROM IDENTIFICATION TO ESCALATION AND REPORTING TO THE BOARD OF DIRECTORS

To ensure that identified IT risks are managed and reported in a tiered manner to the Board of Directors, each disruption is declared according to its BCM Level by the authorized officer: the Branch Manager for BCM Level 4, the relevant Senior Vice President for BCM Level 3, the Technical Director for BCM Level 2, up to the highest level of disruption (BCM Level 1), namely one that impacts the Company's reputation, which is declared and determined directly by the President Director. This structure ensures that the greater the impact of a disruption, the higher the level of officer involved in decision-making, with the Board of Directors serving as the final point of escalation for the most significant risks.

The connection between the technical IT function and the Board of Directors is further strengthened through the IT Steering Committee, which provides recommendations to the Board of Directors on the IT Master Plan and conducts verification prior to its adoption by the Board of Directors, while also serving as the party that approves major changes to the Company's IT systems and infrastructure. Through this series of mechanisms, seven-stage risk management, annual IT audits, semi-annual information security risk assessments, annual DRP testing, tiered BCM escalation up to the President Director, and oversight by the IT Steering Committee, the Company ensures that key IT risks, whether operational, cybersecurity, or disaster-related, are continuously verified on a regular basis rather than remaining static policy.

RESEARCH AND DEVELOPMENT

The Company is currently strengthening its coordination with PT Pelabuhan Indonesia (Persero) to support the development of the National Strategic Area at the Batang Integrated Industrial Estate (KITB). Under this project, the Company is expected to serve as the operator of a multipurpose non-container terminal supporting logistics and distribution activities within the industrial estate.

As a subholding focused on multipurpose terminal services, the Company is preparing operational support through the development of superstructure facilities and information technology systems designed to facilitate integrated cargo handling and port operations.

The terminal is expected to handle various strategic cargoes, including silica sand for the glass industry, steel materials, and gas. The Company is currently conducting internal studies on business potential and operational requirements while engaging in discussions and market outreach with prospective customers as part of the preparations for developing services in the industrial estate.