Corporate digitalisation and cyber security

Corporate digitalisation

During the reporting period, KMG continued its systematic digital transformation targeting improved operational efficiency, business process transparency, and production resilience. The key focus was on establishing end-to-end processes, eliminating fragmented IT solutions, and building a unified digital environment across KMG Group.

Electronic work permits
The Electronic Work Permit module was fully implemented, digitalising the issuance, approval, and monitoring of high-risk work, including work on electrical installations.

The solution enables a fully electronic work permit cycle, with automatic assignment of unique numbers, details completion, built-in format and logic checks, and printable forms that visualise digital signatures for on-site handwritten sign-offs. This delivered a 48% improvement in operational efficiency, a 50% reduction in process steps, and a decrease in paper document flow to 89%.

In December 2025, pilot testing was successfully completed at KazTransOil's head oil pumping station (Pavlodar Oil Pipeline Department), confirming the module's readiness for rollout across KMG Group.

Building and automating an end-to-end procurement process
A project was implemented to build and automate an end-to-end procurement process – from needs identification to payment and supplier performance analysis. The target model brings together key procure-to-pay (P2P) stages within a unified digital framework, from demand planning to contract performance, and integrates with financial and warehouse systems.

Procurement processes (needs identification, market research, and planning) were reengineered, with AS-IS and TO-BE models developed and end-to-end processes established. This resulted in a 56% improvement in process efficiency, a 35% reduction in process steps, and a decrease in paper document flow to 91%.

To support these changes, the Price Marketing, Procurement Planning, and Warehouse Accounting system was enhanced, centralised, and rolled out across KMG Group, with the Procurement Planning module implemented in 13 subsidiaries and associates, and the Price Marketing model in 34 subsidiaries and associates. This eliminated duplicate solutions and established a unified corporate approach to procurement.

The unified digital environment enabled consolidation of data from disparate sources, including historical data, improving pricing, procurement planning, and management decision-making while ensuring transparency and equal supplier access. It also laid the groundwork for further scaling of intelligent procurement tools.

AI assistants were introduced to help create and standardise technical specifications, improving the quality of procurement documentation and reducing errors. A corporate AI assistant (chatbot) for reference information was also implemented, providing quick access to up-to-date procurement regulations and standards.

Migration to SAP S/4HANA
A large-scale project is underway to fundamentally upgrade the ERP landscape through reengineering of key business processes and migration to the SAP S/4HANA platform. The project aims to establish end-to-end business processes, improve operational efficiency and transparency, and ensure complete and reliable data for management decision-making in compliance with regulatory requirements.

The conceptual design phase has been completed, with processes reengineered and a target model based on SAP S/4HANA developed. This has resulted in a 73% improvement in process efficiency, a 20% reduction in the number of steps, and a decrease in paper document flow to 40%.

Work is now underway on system configuration and functionality enhancements, functional and integration testing, and preparations for the pilot launch in 2026.

Inventory of information systems within the corporate architecture
As part of corporate architecture development, KMG compiled a list of business processes for the Corporate Centre and conducted an inventory of information systems across the Group. This analysis is informing the development of a target IT architecture aimed at eliminating duplicate and redundant solutions, optimising the licence portfolio, consolidating maintenance contracts, transitioning to open-source and domestic alternatives, and unifying corporate information systems (covering procurement, HSE, the Transport Management Information System, the Contract Record-Keeping System, the TUMAR Automated Industrial Safety System, the ABAI Information System, the corporate portal, the Learning Management System (LMS), and more). The initiative delivered cost savings of **KZT 844 mln** at the Corporate Centre, with a further **KZT 650 mln** identified as potential savings at subsidiaries and associates. This work is now a continuous activity within the corporate architecture framework development.

HR digitalisation
The approach to HR automation has shifted from fragmented solutions to integrated end-to-end digital processes.

- **System integration:** seamless integration was achieved between the Work.kmg.kz recruitment system and the Team.kmg.kz corporate portal, creating a unified digital environment spanning recruitment, hiring, training, and talent pool planning.
- **Artificial intelligence:** the introduction of AI assistants in recruitment streamlined application processing, improved CV analysis, and strengthened the analytical capabilities of HR departments.
- **Future development:** the launch of a unified HR portal and an audit of 32 priority processes have laid the foundation for the next phase of transformation in 2026.

Automation and standardisation (SAP HCM)
The migration to a paperless working environment was implemented on the SAP HCM (Fiori) platform:
- 41 HR forms were automated (covering leave, business travel, timesheets, and orders);
- electronic digital signatures were introduced for both permanent staff and outstaffed personnel;
- result: significant reduction in operational workload, improved data discipline, and greater process controllability.

Data management: Employee Passport project
A single, reliable source of HR data was created at the level of KMG Group and its subsidiaries and associates:
- integration was established with 1C, SAP, and National Information Technologies systems;
- analytical dashboards and data marts were developed;
- value: management now has a tool for making informed decisions based on verified and comparable data.

Corporate services and employee well-being
Mobile solutions were introduced to enhance the employee support ecosystem:
- **KMG Loyalty and KMG Alem –** apps designed to increase engagement, strengthen the corporate benefits system, and support employee well-being.

Cross-functional solutions
Digitalisation has been extended to key production and logistics chains:

- **transport:** the Transport Management Information System and a railcar tracking system for KTZ have been introduced, delivering end-to-end transparency and eliminating paper-based document flow;
- **production:** refinery operations and contract record-keeping have been automated, reducing operational risks;
- **predictive analytics:** AI models have been integrated into the Dispatch Centre Analytical System to forecast oil product balances, strengthening supply chain resilience and fuel market manageability.

The successful presentation of KMG's digital solutions at the Digital Bridge 2025 international forum testified to the high maturity of the Company's IT landscape and its leadership in applying AI within the oil and gas industry.

These initiatives reflect KMG's systematic approach to digital transformation. The technological foundation now in place will enable the Company to move towards large-scale AI implementation and the development of a unified digital ecosystem for KMG Group in 2026, securing long-term business efficiency and competitiveness.

IT Service Management System (ITSM)
As part of introducing a unified centralised IT Service Management System across the Group, KMG rolled it out to eight subsidiaries and associates, with piloting beginning on 8 October 2025. IT service quality is now centrally monitored across 25 subsidiaries and associates. KMG's Digital Development Department, which oversees information technology, provides over 80 IT services to the Group. The current ITSM system covers:

- 25 subsidiaries and associates, with full control and monitoring of all supported IT services (100% coverage);
- 65 subsidiaries and associates, with established control and monitoring of centralised IT services, including technical support for the electronic document flow (Directum) and Automated Master Data Management systems across KMG Group.

KMG Data
KMG Data is an analytical BI platform for digital reporting, designed for operational monitoring of KMG and its subsidiaries.

The system has a three-tier structure:

- situational module – for tracking key production and corporate indicators, with anomaly and deviation alerts to support management decisions;
- reporting module – for monitoring progress against strategic objectives, key performance indicators, and delivery discipline;
- industry reports – for enabling data analysis and informing recommendations.

Reports developed to date cover:

- financial and production metrics of subsidiaries and associates;
- investment projects;
- travel management;
- financial risks;
- minutes of executive and production meetings;
- SDI – social interaction index with trade unions.

Coverage will be extended to all key production and corporate areas.

Automated Master Data Management project
The Automated Master Data Management (AMDM) system eliminates duplicate entries and enhances planning processes, directly contributing to inventory reduction. Centralised analysis of goods, works, and services, combined with inventory balance monitoring, increases operational efficiency and supports more informed decision-making. The system also maintains a centralised directory of business partners (counterparties). In 2025, KMG upgraded to AMDM 2.0. The project is now complete, with the system operational at KMG's Corporate Centre and across 34 subsidiaries and associates for the goods, works, and services directory, and across 36 subsidiaries and associates for the business partner directory. Further functionality expansion and wider subsidiary and associate coverage are under consideration.

AI Assistant project
KMG's AI assistant portfolio comprises specialised digital solutions that automate routine business processes, support content creation and analysis, generate analytical recommendations, function as intelligent chatbots, and automate the minute-taking of meetings.

The portfolio includes the following solutions:

- collective bargaining agreement assistant – for centralised search and data extraction from subsidiary and associate collective bargaining agreements;
- legal assistant – for searching across KMG's regulatory documents, with analytical capabilities for decision analysis and justification;
- meeting minutes assistant – for automatically recording action items, assigning responsibilities, and setting deadlines from online meetings;
- procurement assistant – for analysing technical specifications and comparing functional characteristics of proposed options to optimise procurement.

Key AI assistants are in the final stages of preparation for deployment within the Corporate Centre, with subsequent rollout and scaling to subsidiaries and associates planned.

HSE digitalisation

- **QR tagging:** key equipment is being fitted with QR codes providing instant access to technical documentation and inspection history. The system automatically notifies when scheduled checks are due, preventing operation of faulty equipment.

Safety culture

- **LOTO (Lockout/Tagout):** standards for locking out hazardous energy sources have been introduced, physically preventing accidental equipment start-up during maintenance.
- **Training:** interactive Danger Zone 3D courses have been introduced as mandatory training standard for all employees and contractors.

Cyber security

KMG's information security goals remain ensuring reliable asset protection from external and internal threats, preventing financial and reputational losses, and minimising damage from cyber attacks to maintain uninterrupted operations across KMG and its subsidiaries and associates.

Information security is an ongoing process that adapts to the evolving threat landscape. Given the increasing aggressiveness of the cyber environment in 2025, continuous analysis, audits, and infrastructure security testing are critically important. The large-scale digitalisation of production processes across the extensive structure of complex oil and gas facilities requires particular vigilance, as disruption to technological cycles can have irreversible consequences for both the Company and the national economy. No incidents with critical impact on KMG's production and business continuity occurred during the reporting period.

To achieve its goals, KMG rigorously complies with Kazakhstan's laws and adheres to global best practices. In October 2025, the Company successfully passed a recertification audit by TÜV Rheinland, confirming its Information Security Management System's compliance with ISO/IEC 27001:2022. This attests to the maturity of the Company's processes and demonstrates to stakeholders KMG's commitment to global data security standards.

The information security perimeter covers corporate IT infrastructure, critical information and communication components, and automated process management systems.

Risk assessment and threat monitoring are carried out continuously through the Information Security Operations Centre. In 2025, the load on protective systems increased manifold. Over the 12-month reporting period, the Information Security Operations Centre identified and resolved 2,026 confirmed incidents.

KMG regularly conducts independent cyber resilience assessments, including periodic penetration tests by various cyber security teams to objectively evaluate perimeter security. As part of advancing KMG's defence strategy, Red Teaming techniques are being introduced to identify hidden attack vectors.

The Company prioritises developing a cyber security culture and human-centric protection. All employees now complete training on a specialised platform, with a targeted approach automatically assigning modules to address knowledge gaps identified during practical assessments.

The SOC[1] team runs regular phishing simulations, including those using reverse psychology techniques. A large-scale awareness campaign using neutralised malware (with controlled C2 connectivity) enabled staff to safely experience real-world targeted attack scenarios.

The Company proactively manages cyber threats by implementing innovative technologies. In 2025, several pilot projects were successfully implemented, and preparations began for migrating to an extended detection and response (XDR)[2] system with AI elements. The Zero Trust concept is being actively developed: Privileged Access Management[3] coverage has been expanded, daily rotation of local administrator passwords[4] introduced, and data encryption (BitLocker via TPM[5]) strengthened.

Thanks to this layered defence, KMG repelled over 16 million cyber attacks on its web resources over the 12 months of 2025, reflecting both a manifold increase in external pressure and the high effectiveness of deployed protections.

KMG's management views information security as integral to corporate governance, contributing to the Company's sustainable development and innovative growth.

Looking ahead, KMG will continue to advance its digital sovereignty, refine its Zero Trust strategy, and enhance staff expertise, all in strict compliance with Kazakhstan's laws and international security standards.

1 The Security Operations Centre (SOC) – a dedicated cyber security team providing 24/7 monitoring of IT infrastructure to detect, analyse, and respond to cyber incidents, safeguarding the business against attacks, reducing risks, and maintaining business continuity.
2 Extended Detection and Response (XDR) – a comprehensive cyber security solution that aggregates and analyses data across multiple layers of IT infrastructure to proactively detect, investigate, and automatically respond to sophisticated cyber threats.
3 Privileged Access Management (PAM) – a set of information security solutions for controlling, monitoring, and protecting accounts to prevent data breaches, misuse, and cyber attacks, while ensuring compliance with regulatory requirements.
4 LAPS – Local Administrator Password Solution.
5 Trusted Platform Module (TPM) – the most secure and convenient technology for disk encryption.