Our Performance continued

06 Drive Robust Governance and Responsible Operations

alinma is a trusted steward of personal and commercial financial activity, operating within a financial landscape that is becoming more complex as a result of regulatory intensity, technological disruption, and changing market forces. To meet this responsibility, ethical conduct and accountability are deeply embedded in our governance framework, with integrity underpinning our Shariah-compliant culture.

In line with leading international governance practices, we focus on strong regulatory compliance, effective anti-money laundering and anti-corruption controls, resilient risk and business continuity management, and advanced cybersecurity capabilities. These priorities are overseen by a seasoned Board of Directors and executive leadership team within a well-defined organizational structure.

Governance, accountability, transparency, and ethics

alinma is governed by a highly experienced Board of Directors responsible for setting vision, strategic direction, and oversight of sustainability, with appointments made in line with regulatory requirements. Comprised entirely of non-executive and independent members, the Board is structured to ensure objective, transparent decision-making, supported by strict rules to prevent conflicts of interest. This independent oversight enables rigorous scrutiny of Management and promotes strong governance that underpins long-term trust and sustainable growth. In 2025, we were pleased that Ms. Maram Mohammed Alnumay joined the Board, bringing gender diversity and a fresh perspective to the Bank.

As part of its overall supervisory duties, the Board takes sustainability-related issues like governance, risk management, compliance, and long-term strategic objectives into account. alinma arranges comprehensive sustainability training for the Board to enhance ESG capability at this highest level and sustainability metrics are included in the Board's performance evaluation.

alinma's standards for ethical behavior and professional conduct are set out in its Code of Conduct. The Code applies across the organization, from the Board of Directors to employees and suppliers. We place special emphasis on avoiding conflicts of interest through a comprehensive governance framework that requires clear disclosures, Board oversight, and the exclusion of conflicted parties from decision-making, with independent review and approvals applied where required. Related-party transactions are governed by a dedicated framework to ensure arm's-length terms, supported by centralized disclosure, layered approvals, and transparent reporting to regulators to maintain fairness and regulatory compliance.

Sustainability elements were integrated into the Code of Conduct in 2025, with all employees signing agreement to the Code. This allows us to reinforce ethical decision-making, promote consistent standards of behavior across the organization, and ensure sustainability considerations are embedded in everyday business practices.

In 2025, alinma updated the Bank's whistleblowing policies and procedures to strengthen Stakeholder reporting of improper, unethical, or inappropriate behavior within the Bank.

alinma's compliance approach is centered on full adherence to applicable laws, regulations, and internal policies, while embedding a strong compliance culture across all business and control functions. Compliance is viewed as a shared responsibility, led by the Board and Senior Management and extended to every employee, and is reinforced through an annual risk-based compliance plan and ongoing review of policies to ensure regulatory alignment. In 2025, we raised employees' awareness and institutional knowledge of SAMA regulations and instructions through the alinma Rule Book Portal, a centralized database published on our intranet. In addition, our new Regulatory Compliance Portal streamlines compliance-related requests and responses through automation, clear workflows, and easy request tracking and management.

Business continuity

In 2025, we strengthened business continuity by aligning our program with strategic objectives, heightened regulatory expectations, and operational resilience requirements, while actively managing third-party risks and adapting to digital transformation, including AI. In line with SAMA guidance, alinma conducted disaster recovery drills, crisis simulations, and quarterly readiness exercises, confirming that plans, procedures, and response capabilities were effective and well understood.

We implemented safeguards to maintain the availability of vital services in the event of unforeseen interruptions, such as online and mobile banking, ATMs, and payment gateways. alinma governs business continuity through a structured framework aligned with the Bank's 2025 strategy, the SAMA BCM Framework and ISO standards, using incidents, tests, and regulatory changes to continuously strengthen the program. Active-active data centers and disaster recovery sites enable uninterrupted customer access and flexible working arrangements during physical incidents, while reducing travel requirements and supporting both operational resilience and ESG objectives.

ESG risk management

We acknowledge that ESG risks can materially affect financial results, reputation, and regulatory compliance, and we actively manage these risks across our operations. In line with this, the Bank has already begun embedding ESG considerations into alinma's risk management framework in a structured and phased roadmap approach, in close coordination between the risk management and sustainability functions, supporting sustainable growth and long-term value. Potential ESG risk factors affecting the Bank or its customers are identified and assessed using ESG scoring, scenario analysis, and relevant global frameworks. In the year under review, we published an ESG risk framework, establishing a structured and consistent approach to identifying, assessing, and managing ESG risks across the Bank.

Data privacy and cybersecurity

alinma manages data privacy through a centralized and clearly defined operating model. Oversight is assigned to the Data Protection Officer, while the Data Privacy Unit, operating under the Enterprise Data Management Department, manages day-to-day execution and control. This ensures consistent application of data protection requirements, effective monitoring of compliance, and timely response to data privacy risks across the organization. Similarly, alinma manages cybersecurity through a centralized and clearly defined operating model. Oversight is assigned to the Chief Information Security Officer (CISO), while the Cybersecurity Department manages day-to-day execution, monitoring and enforcement of security controls. This structure ensures the consistent implementation of cybersecurity policies and standards, effective monitoring of compliance with regulatory and internal security requirements, and a timely response to cyber threats and vulnerabilities across the organization.

During 2025, we made significant progress in strengthening the data privacy framework. We enhanced and finalized core privacy policies, standards, and procedures in close collaboration with cybersecurity, procurement, and other control functions. The Bank also reinforced contractual governance by strengthening privacy clauses, data processing agreements, and third-party oversight. In parallel, alinma managed evolving regulatory and supervisory requirements, maintaining alignment with the Personal Data Protection Law (PDPL), its Implementing Regulations, and SAMA expectations. We further improved efficiency and traceability by engaging a specialized vendor to automate core data privacy business-as-usual processes. Together, these actions advanced governance maturity and strengthened operational resilience.

Data privacy controls are tested regularly through internal reviews conducted by Compliance and Internal Audit, as well as external regulatory and supervisory assessments by SAMA and independent auditors. These reviews provide objective assurance over the effectiveness of the Bank's data privacy governance and controls. No personal data breaches were identified in 2025.

View the alinma Bank Privacy Policy here:

During 2025, 112 data privacy awareness and training activities were delivered as part of alinma's broader compliance and governance programs. These activities focused on enhancing employee awareness of PDPL obligations, responsible data handling practices, and core privacy principles.

alinma significantly strengthened its cybersecurity capabilities in 2025 through the establishment of a Cybersecurity Defense Center that provides 24/7 monitoring and incident response, processing more than 72,000 security alerts quarterly. The Bank also enhanced threat detection by building a centralized security data lake, enabling advanced analytics and future AI-driven security use cases, while Cyber Threat Intelligence operations handle over 11,900 intelligence alerts quarterly to support proactive threat detection.

In parallel, alinma continues to strengthen risk management by conducting regular cybersecurity risk assessments, penetration testing, vulnerability testing and architecture reviews to ensure secure technology deployment. The Bank maintains strong regulatory alignment through certifications such as ISO 27001, PCI DSS and SWIFT, alongside compliance with SAMA, NCA and CMA cybersecurity requirements. In addition, the cybersecurity team actively promotes a security-first culture by delivering continuous cybersecurity awareness campaigns and training sessions across the organization. These initiatives are further supported by strong governance, continuous policy enhancement and a forward-looking Cybersecurity Strategy for 2026–2028.