data privacy and information management

alrajhi bank regards data as a core enterprise asset that drives operational excellence, informed decision-making, and superior customer experiences. To protect this asset, the bank applies rigorous data governance, privacy, and security standards, ensuring that all regulatory and industry expectations are met. Responsibility for data privacy lies with the Chief Digital Officer, while the Chief Risk Officer oversees cybersecurity activities. Oversight is further strengthened by the Cyber and Information Security Committee, which guides implementation, governance and continuous monitoring of all related programmes.

The bank's Data Governance Policy, established in 2022, provides an end-to-end framework across 14 essential domains, ranging from data quality, architecture, metadata and analytics to data sharing, open data, and personal data protection. This policy supports consistent data management practices, promotes regulatory alignment, and reinforces a unified governance model across the organisation.

Following the introduction of Saudi Arabia's first Personal Data Protection Law (PDPL) in 2023, the bank collaborated with the National Data Management Office (NDMO) and adhered to SAMA guidelines to embed robust personal data controls. Throughout the reporting year, the bank catalogued all personal data processing activities, assessed their potential impact on individuals, and built a centralised repository for documenting data processing operations. alrajhi bank also completed a compliance assessment of data subject rights to ensure alignment with all data protection requirements.

In 2024, the bank implemented its updated Privacy Policy and introduced a detailed Privacy Notice that complies with PDPL and NDMO standards. This Notice explains the types of data collected, the purpose of data usage, and how data is managed throughout its lifecycle. It also outlines customer rights, including the ability to revoke consent for personal data processing at any stage.

The bank maintains a formal Data Breach Management procedure, aligned with Article 20 of the PDPL Law and Article 24 of its regulations. These require reporting any confirmed breach to SAMA within four hours and to SDAIA within seventy-two hours, as well as notifying impacted individuals without delay. The process includes breach detection through monitoring controls, investigation, impact evaluation, remediation and restoration activities, and timely reporting.

Both internal and external privacy policies have been updated and embedded across the institution to reflect PDPL and alrajhi bank standards. While a formal AI governance framework is still under development, the bank has carried out privacy assessments to identify sensitive data risks and strengthen controls accordingly. Compliance is continuously evaluated against PDPL and NDMO requirements across all jurisdictions where alrajhi bank operates.

The Data Privacy Policy applies to all internal and external parties, including employees, contractors, vendor personnel, and subsidiary staff, who handle personal data on behalf of the bank, whether through manual processes or automated systems. The policy is fully aligned with PDPL and NDMO standards.

Cybersecurity remains a foundational pillar of alrajhi bank's operational resilience and governance framework. As cyber threats continue to evolve globally, the bank maintains a comprehensive and structured cybersecurity risk management approach to safeguard its information assets, systems, and business processes. Cybersecurity at alrajhi bank is built on three core principles:

- Confidentiality – ensuring information is accessible only to authorised individuals
- Integrity – maintaining accuracy and reliability of data
- Availability – ensuring information and systems remain accessible when required

alrajhi bank's Cybersecurity Policy complies with regulatory requirements from governing bodies like SAMA Cybersecurity strategy and framework, SARIE, NCA (National Cybersecurity Authority), In addition to, standard best practices like ISO 27001, Payment card industry- data security standard (PCI-DSS). All employees must comply with the bank's Cybersecurity Policy and related frameworks, standards, processes, and guidelines. The Information Security Department (ISD) oversees periodic reviews of the Policy to ensure ongoing compliance with legal, regulatory, and contractual requirements. Adherence is mandatory, and violations are subject to disciplinary measures. Exception or waiver requests must be formally submitted with justification, reviewed for risk and compliance implications, and approved through defined governance channels. Requests concerning SAMA Cybersecurity Framework requirements follow the established SAMA waiver procedure.

Continuous cybersecurity risk assessments are conducted across internal environments and third-party engagements to identify, evaluate, and prioritise risks based on severity. Risk treatment plans are fully aligned with the bank's enterprise risk management framework, ensuring informed decision. Governance is overseen by the Board of Directors, supported by the Cybersecurity Committee, which includes senior executives, the MD & CEO, and functional leaders. This Committee provides strategic guidance, monitors cybersecurity programmes, reviews key risk and performance indicators, and ensures that cybersecurity initiatives align with the bank's risk appetite. The bank continues to invest in strengthening its cybersecurity function through a clearly defined organisational structure and ongoing workforce capability assessments, ensuring the availability of qualified cybersecurity professionals across all business units and subsidiaries.

Cybersecurity controls and monitoring

To enhance threat detection and response capabilities, alrajhi bank has implemented advanced security monitoring tools integrated across its technology landscape. All security events and potential breaches are logged and managed through a dedicated case management system and handled according to the bank's predefined incident response playbooks. Incidents are classified using the bank's data classification matrix, which determines escalation thresholds. High and critical incidents result in activation of the Crisis Management Team for coordinated containment and recovery. Each incident undergoes root-cause analysis, eradication, and a formal lessons-learned review to strengthen future preparedness.

Cybersecurity culture and awareness

Building a cyber-aware workforce is integral to the bank's cybersecurity strategy. It is mandatory for all new employees to complete mandatory cybersecurity onboarding modules developed in partnership with alrajhi Academy. An annual cybersecurity awareness training plan is delivered to all staff, complemented by periodic awareness campaigns to reinforce secure behaviour and cultivate a resilient cybersecurity culture throughout the organisation.

Technical assessments and testing

The bank conducts regular vulnerability assessments (VA) and penetration testing (PT) on its systems and applications, supplemented by ad-hoc assessments based on emerging threats. All findings are communicated to relevant owners and tracked until closure, with oversight from senior management to ensure timely and effective remediation.

Vendor and third-party cybersecurity compliance

Given the increasing reliance on third-party service providers, alrajhi bank enforces stringent cybersecurity requirements within its procurement and vendor management processes. Contracts include comprehensive clauses covering data confidentiality, integrity, availability, incident response responsibilities, and breach notification procedures. Vendors must demonstrate robust security controls, maintain relevant certifications such as ISO standards, and allow the bank to conduct security assessments to validate compliance.

Identity and access management

The bank employs Identity and Access Management (IAM) processes to ensure secure and authenticated access across the bank's environment. IAM systems are integrated with Active Directory and LDAP for centralised user authentication and access governance. In the event of a data breach, the cybersecurity and data privacy teams coordinate to assess the impact, implement corrective measures, and complete all regulatory and customer notifications as required.

Commitment to customer trust and institutional resilience

Cybersecurity is essential to maintaining customer trust, protecting sensitive information, and upholding compliance, reputation, and shareholder confidence. The Board and Executive Management remain strongly committed to supporting the bank's cybersecurity strategy, policies, and objectives. Through its comprehensive controls, governance mechanisms, and continuous investments in people and technology, alrajhi bank ensures strong cybersecurity compliance and resilience, securing its digital assets and enabling safe, uninterrupted banking services for all customers.