Kiteworks

GUIDE

Kiteworks' Guide to Saudi Arabia NDMO Standards

Securing Government Data With Advanced File Sharing and Governance

Introduction

The Saudi Arabia National Data Management and Personal Data Protection Standards represent a comprehensive regulatory framework established by the National Data Management Office (NDMO) to govern data management practices across the Kingdom. Issued in January 2021 as Version 1.5 under Cabinet Resolution 292, these standards serve as the foundational blueprint for implementing effective data governance and personal data protection measures throughout Saudi Arabia's public sector entities. The regulation aligns with Saudi Arabia's Vision 2030 initiative, which seeks to modernize government operations, enhance transparency, and build a data-driven economy based on international best practices.

The standards apply to all public entities within the Kingdom of Saudi Arabia, including independent governmental organizations, public authorities, and their affiliates. The scope extends beyond direct government agencies to encompass any company that operates public utilities, maintains national infrastructure, or provides public services related to such infrastructure. Business partners handling government data also fall under these requirements and must understand and apply the standards to all government data assets within their control and custody. The regulation covers government data in all forms, including paper records, emails, electronic data, voice recordings, videos, maps, photos, scripts, handwritten documents, and any other recorded information format.

The framework encompasses fifteen distinct domains that span the complete data lifecycle from creation to retirement. Data Governance provides the authority and control over planning and implementation of organizational data management practices through people, processes, and technologies. Data Catalog and Metadata focuses on enabling effective access to high-quality integrated metadata through automated data catalog tools. Data Quality concentrates on improving organizational data quality to ensure data remains fit for purpose based on consumers' requirements. Data Operations focuses on designing, implementing, and supporting data storage to maximize data value throughout its lifecycle. Document and Content Management involves controlling the capture, storage, access, and use of documents and content stored outside relational databases. Data Architecture and Modeling establishes formal data structures and data flow channels to enable end-to-end data processing. Reference and Master Data Management links all critical data to single master files, providing common reference points for all critical data. Business Intelligence and Analytics focuses on analyzing organizational data records to extract insights and draw conclusions. Data Sharing and Interoperability involves collecting data from different sources through integration solutions that foster harmonious communication between IT components. Data Value Realization continuously evaluates data assets for potential data-driven use cases that generate revenue or reduce operating costs. Open Data focuses on organizational data that can be made available for public consumption to enhance transparency and foster economic growth. Freedom of Information provides Saudi citizens access to government information while establishing processes for information access and dispute resolution. Data Classification involves categorizing data so it may be used and protected efficiently through systematic classification levels. Personal Data Protection focuses on protecting subjects' entitlement to proper handling and nondisclosure of their personal information.

Data Security and Protection encompasses processes, people, and technology designed to protect entity data, including authorized access controls and safeguarding against unauthorized disclosure.

Each domain contains specific controls and 191 detailed specifications that organizations must implement according to a three-year phased approach based on priority levels. Organizations face significant compliance risks under these standards. The NDMO conducts annual compliance assessments using a binary pass-fail system for each specification, with scores cascading from specification level to control, domain, and overall entity levels. Noncompliance can trigger ad hoc audits and corrective actions. The regulation requires Chief Data Officers to lead compliance efforts and provide evidence-based reporting to demonstrate adherence. Entities must establish comprehensive data management offices, implement specific organizational roles, and maintain detailed registers of their data governance decisions and activities.

The standards complement other Saudi Arabian data protection regulations, including the Personal Data Protection Law (PDPL) enacted in March 2022, which governs personal data processing across all sectors. The National Cybersecurity Authority oversees the Data Security and Protection domain, while sector-specific regulations from entities like the Saudi Central Bank and Ministry of Commerce address specialized data protection requirements. Organizations operating within Saudi Arabia's regulatory environment must align their data management practices with these interconnected frameworks to achieve comprehensive compliance and support the Kingdom's digital transformation objectives.

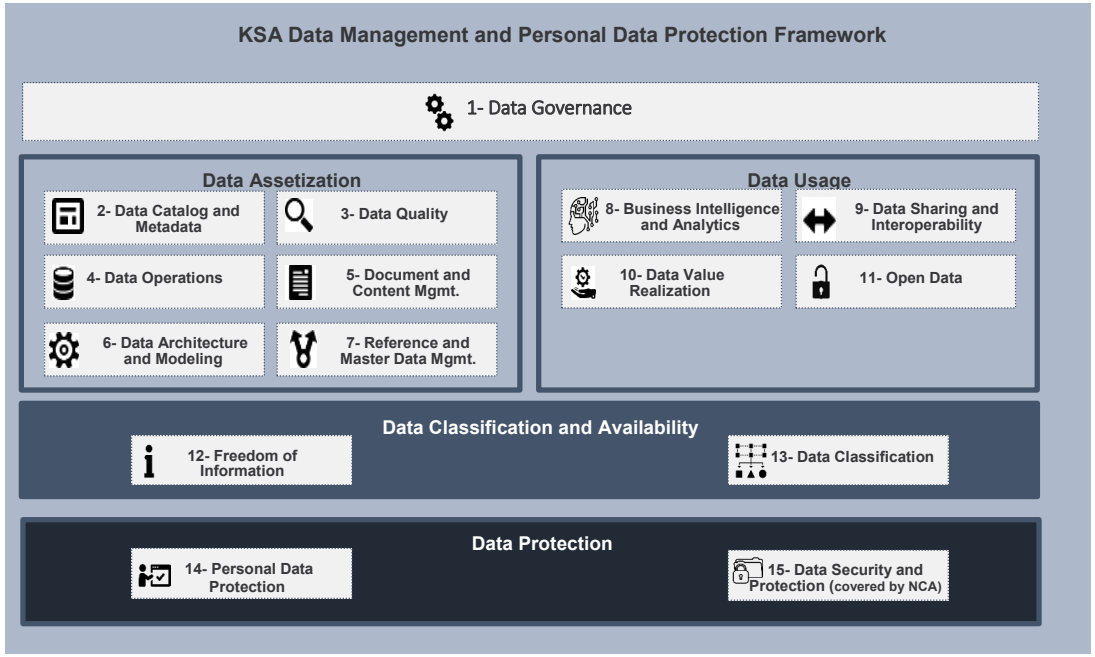

Figure 1: KSA Data Management and Personal Data Protection Framework

The Kiteworks Secure File Sharing and Governance Platform

The Kiteworks Private Data Network empowers organizations to share sensitive data with trusted parties by email, file sharing, file transfer, and other channels at the highest levels of security, governance, and compliance while maintaining full visibility and control over their file sharing activities. The Kiteworks platform provides:

Protection of Unstructured Data

Kiteworks provides comprehensive protection for unstructured data through its advanced firewall and zero-trust file sharing capabilities that ensure sensitive unstructured data remains secure throughout its life cycle, whether at rest or in transit across various communication channels.

Governance and Compliance

Kiteworks reduces compliance risk and cost by consolidating advanced data governance capabilities into a single platform. Whether employees send and receive data via email, file share, automated file transfer, APIs, or web forms, it's covered.

Simplicity and Ease of Use

Kiteworks offers a user-friendly interface that simplifies secure file sharing and collaboration, enabling users to easily send, receive, and manage sensitive data without compromising security. The platform's intuitive design and seamless integration with existing workflows ensures high user adoption rates and minimizes the learning curve for organizations implementing robust data protection measures.

The Kiteworks Platform and Saudi Arabia National Data Management and Personal Data Protection Standards

Data Governance Domain

Data Governance provides the authority and control over the planning and implementation of organizational data management practices through people, processes, and technologies. This domain ensures consistent and proper handling of data assets in alignment with the entity's Data Management and Personal Data Protection Strategy, establishing foundational oversight for all data-related activities.

Control Specifications	Kiteworks Solution
Control ID DG.8 of the Data Governance Domain requires entities to implement comprehensive documentation and version control systems for data governance materials. Organizations must establish a Data Governance Approvals Register to document and track all CDO-approved decisions with their justifications. Additionally, they must maintain a Data Management Issue Tracking Register containing historical records of data management problems and resolutions raised by users. Finally, entities must implement formal version control processes for all data management documents and artifacts they create, ensuring proper change management and document integrity throughout the governance lifecycle.	Kiteworks partially supports compliance with Saudi NDMO Control ID DG.8 through its comprehensive tracking and audit capabilities. The platform maintains detailed audit logs which include date, user, activity, and IP address for every entry. Kiteworks implements robust version control through its file versioning system that tracks all changes to documents, maintaining complete version histories. The system's consolidated, normalized logging ensures all governance decisions and document modifications are properly documented and retrievable for compliance auditing purposes.

Data Catalog and Metadata Domain

Data Catalog and Metadata focuses on enabling effective access to high-quality integrated metadata through automated data catalog tools. This domain serves as the single point of reference for organizational metadata, supporting data discovery, understanding, and management by providing comprehensive information about data assets and their characteristics.

Control Specifications	Kiteworks Solution
Data Catalog and Metadata Domain requirements mandate entities to implement comprehensive technical controls centered around an automated Data Catalog tool that serves as the central metadata management system. Organizations must establish automated workflows for metadata population, updates, and quality management, including processes for handling user annotations, tags, and trust certificates within the catalog system. Technical implementations require automated notification systems to alert users of metadata changes, comprehensive audit trail capabilities that track all user activities and operations within the catalog, and systematic version management to ensure the Data Catalog tool remains current with vendor releases. All processes must include defined SLAs for issue remediation and follow NDMO Data Catalog Guidelines for standardized implementation across Saudi Arabian public entities.	Kiteworks supports Data Catalog and Metadata Domain compliance through its comprehensive consolidated activity logging system that captures all necessary metadata with key-value pairs for every tracked activity, including dates, users, activities, and IP addresses. The platform manages file metadata through its Private Data Network supporting versioning, comments, and both MIP and custom tags, and standard file metadata such as creation and modification dates, file types, etc. Kiteworks can export these reports via csv and API integrations for review and data storage. Kiteworks provides automated notifications for real-time metadata change monitoring and certificate-based authentication with automatic OCSP/CRL handling and advance expiration notifications. The system's attribute-based access control policies classify data assets contextually, while comprehensive audit capabilities track all user logins and operations without data throttling. One-click updates through the hardened virtual appliance ensure current tool versioning with cryptographic verification and secure offline update processes for air-gapped deployments.

Data Operations Domain

Data Operations focuses on the design, implementation, and support for data storage to maximize data value throughout its lifecycle from creation/acquisition to disposal. This domain encompasses database management, storage optimization, backup and recovery procedures, and performance monitoring to ensure reliable and efficient data operations.

Control Specifications	Kiteworks Solution
Data Operations Domain Control DO.3 requires entities to implement comprehensive database operations management with robust technical controls. Organizations must establish continuous database monitoring systems that track capacity utilization, availability metrics, query execution performance, and configuration changes for root cause analysis. Technical requirements include role-based access control systems aligned with data classification standards, comprehensive storage configuration management with change control processes, and configuration auditing capabilities. Entities must maintain current DBMS versioning with documented update strategies and implement performance-based Service Level Agreements specifying availability timeframes, transaction execution limits, and escalation procedures. All database operations require detailed tracking and reporting mechanisms to ensure operational compliance and performance optimization.	Kiteworks provides comprehensive monitoring capabilities. Logged activities may be viewed for the entire system, administrative actions, a specific user, a specific file or folder, or a specific form and log entries provide additional key-value pairs containing metadata related to the specific activity tracked. The system supplies built-in reports of system usage metrics, within a specified period. The comprehensive version management Kiteworks provides through its one-click update system allows the hardened virtual appliance to check for updates, and a system admin can click to download, cryptographically verify, and apply the update to the cluster automatically. This updates the entire solution, including the operating system, databases, web servers, Kiteworks application code, and any other services, in a single step. Additionally, Kiteworks provides a secure offline update process for deployments that are air gapped or have no internet access.

Document and Content Management Domain

Document and Content Management involves controlling the capture, storage, access, and use of documents and content stored outside of relational databases. This domain establishes processes for managing unstructured information, implementing digitization initiatives, and ensuring proper lifecycle management of organizational documents and multimedia content.

Control Specifications	Kiteworks Solution
Data and Content Management Controls DCM.4.4 and DCM.4.5 require entities to implement comprehensive document management automation with integrated metadata publishing capabilities. Technical controls mandate publishing document metadata to Data Catalog systems following established metadata management processes. Organizations must deploy Document Management Systems with OCR functionality, document indexing, version control with change history tracking, secured access controls, global search capabilities, and workflow development tools. Additional requirements include Web Content Management Systems for portal content and collaboration platforms enabling real-time document editing, chat communication, and change tracking. These integrated systems must provide complete document lifecycle management with automated metadata population and comprehensive search and discovery functionality across all document repositories.	The platform provides file storage capabilities and comprehensive file versioning that tracks document changes over time, supporting the versioning requirement. Kiteworks implements secured access to documents through role-based access controls with Owner, Manager, Collaborator, Downloader, and Viewer roles. The system offers collaboration capabilities where users can share folders and files, with tracking of who accessed or modified documents.

Data Architecture and Modeling Domain

Data Architecture and Modeling focuses on establishment of formal data structures and data flow channels to enable end-to-end data processing across and within entities. This domain defines conceptual, logical, and physical data models while creating architectural frameworks that support efficient data integration and system interoperability.

Control Specifications	Kiteworks Solution
Data Architecture and Modeling controls DAM.4.2 and DAM.7.1 require entities to implement comprehensive technical toolsets for data architecture design, development, and implementation initiatives. Technical controls mandate selecting and deploying integrated technology platforms covering data architecture design with visual representation capabilities, data modeling tools with drawing functionality for creating and modifying data objects and relationships, and data lineage capabilities for capturing and maintaining data flows between systems to enable impact analysis. Additionally, organizations must establish Data Architecture and Modeling Registers to systematically store and maintain all data and technical architecture project documentation, reference materials, and data model designs for comprehensive governance and compliance tracking.	Kiteworks is not a relational modeling system, instead it manages unstructured data (files). Kiteworks enables flexible user-defined hierarchical folder structures with hierarchical access control permissions. The platform provides data lineage and visualization capabilities. The Repositories Gateway enables data lineage tracking by making external data sources appear as integrated folders, providing visibility into data flows between systems. The CISO Dashboard supports data architecture requirements by offering real-time and historical views of all inbound and outbound file movement, showing comprehensive activity of data transfers including who's sending what to whom, when, and where. The dashboard provides export capabilities to spreadsheets for further analysis and maintains comprehensive activity logs for files, folders, and systems.

Open Data Domain

Open Data focuses on the organization's data that could be made available for public consumption to enhance transparency, accelerate innovation, and foster economic growth. This domain establishes processes for identifying, preparing, and publishing datasets that benefit citizens and support government accountability while maintaining appropriate security controls.

Control Specifications	Kiteworks Solution
Open Data controls OD.3.3 and OD.3.6 require entities to implement comprehensive open data publishing and maintenance systems with robust technical capabilities. Technical controls mandate publishing datasets under the KSA Open Data License following NDMO regulations, with automated systems for regular dataset updates and metadata documentation whenever changes occur. Organizations must establish continuous review mechanisms to ensure ongoing regulatory compliance, implement data traceability systems that document data provenance, and maintain comprehensive versioning history for all published datasets. These controls require integrated publishing platforms with change tracking, metadata management, compliance monitoring, and historical versioning capabilities to ensure transparent and accountable open data governance throughout the dataset lifecycle.	Kiteworks provides partial support through its comprehensive versioning, audit logging, and access control capabilities. The platform maintains detailed file versioning that tracks all changes to datasets over time, supporting versioning history requirements for published open datasets. Kiteworks' comprehensive audit logging system captures date, user, activity, and IP address for all operations, enabling documentation of data provenance and change tracking. The system's role-based access controls with Owner, Manager, Collaborator, Downloader, and Viewer roles can support data access requirements, while geofencing and IP address controls enable appropriate access restrictions. File expiration and time-based controls support dataset lifecycle management.

Data Classification Domain

Data Classification involves the categorization of data so that it may be used and protected efficiently. Data Classification levels are assigned following an impact assessment determining the potential damages caused by the mishandling of data or unauthorized access to data, ensuring appropriate security measures match sensitivity levels.

Control Specifications	Kiteworks Solution
Data Classification controls DC.3.1 and DC.3.5 require entities to implement comprehensive data identification and classification metadata management systems. Technical controls mandate identifying and inventorying all organizational datasets and artifacts as part of the Data Classification Implementation process following NDMO regulations. Organizations must utilize Data Catalog automated tools for systematic dataset and artifact inventory management when available. Additionally, entities must publish all assigned classification levels as metadata within the Data Catalog system, executing metadata population according to established Metadata and Data Catalog Management domain processes. These controls require integrated classification systems with automated inventory capabilities, metadata publishing functionality, and seamless integration between data identification processes and catalog management systems.	Kiteworks provides partial support for Data Classification controls DC.3.1 and DC.3.5 through its comprehensive data asset management capabilities. The platform provides asset management for data assets by classifying them in the context of a data-centric risk policy and supports attribute-based access control (ABAC) policies that can classify data based on folder paths, MIP sensitivity labels, and custom tags. Kiteworks can define and enforce data access policies based on MIP tags in imported files. Kiteworks maintains consolidated activity logs that inventory all system data assets and tracks classification-related activities.

Data Security and Protection Domain

Data Security and Protection encompasses processes, people, and technology designed to protect entity data, including authorized access controls, spoliation prevention, and safeguarding against unauthorized disclosure. This domain falls under the National Cybersecurity Authority's mandate and addresses comprehensive information security requirements.

Control Specifications	Kiteworks Solution
Data Security and Protection controls DS.3, DS.4, DS.7, and DS.8 require entities to implement comprehensive information security frameworks with integrated technical controls. Organizations must establish minimum security provisions during system development, testing, and implementation phases, including secure development lifecycle processes. Technical controls mandate robust identity and access management systems for authenticating users and information systems requesting access to organizational assets. Entities must maintain documented inventories of all information assets containing critical data with comprehensive asset management capabilities. Additionally, organizations must implement operational security management systems enabling personnel to continuously monitor, assess, and protect information assets through systematic operational duties and security oversight mechanisms throughout the information security lifecycle.	Kiteworks provides support for Data Security and Protection controls through its robust security framework. For DS.3, the Kiteworks implements comprehensive DevSecOps with "shift left" security practices, including security training, design reviews, secure code reviews, and automated testing throughout development. DS.4 requirements are addressed through extensive identity and access management supporting multiple authentication methods including SAML 2.0, LDAP, multi-factor authentication, and certificate-based authentication with role-based access controls. For DS.7, Kiteworks provides asset management capabilities that classify and inventory data assets using attribute-based access control policies. DS.8 operational security management is supported through comprehensive audit logging, real-time monitoring, intrusion detection systems, automated notifications, and continuous security information feeds to SIEM systems, enabling personnel to monitor, assess, and protect information assets effectively.