

AVIATION · DATA & AI GOVERNANCE



Continuous data and AI trust, not periodic compliance.

How Saudi Arabia's new national carrier is standing up the data and AI trust foundation the rest of the airline is built on.



What this is about.

Riyadh Air, Saudi Arabia's new national carrier, is being built from a clean technology foundation. That foundation had to satisfy the fourteen domains under the National Data Management Office, meet obligations under the Personal Data Protection Law, and enable AI across commercial, operations, and guest experience.

The program was shaped by a structural choice: build governance authority before writing the policies it would enforce, prove the operating model on a single Division before scaling it across the airline, and let AI governance stand up alongside the core NDMO work rather than trail behind it.

“For Riyadh Air, data and AI trust is not just a compliance requirement. It is part of the foundation we are building as a new national carrier. The goal is to operationalize governance early, so the evidence, controls, and accountability are already part of how the business runs.”

HEAD OF DATA AND AI GOVERNANCE, RIYADH AIR

The regulatory reality.

Saudi Arabia's National Data Management Office publishes a data management maturity framework covering fourteen domains. Entities operating within the Kingdom's regulated data ecosystem are expected to meet these standards, with progress measured through periodic assessments. The Priority 1 controls form the enforcement baseline, and the consequences of missing them extend well beyond paperwork.

The Personal Data Protection Law, enforced by the Saudi Data and AI Authority, governs how personal data is collected, processed, and moved within the Kingdom and across its borders. Enforcement started in 2024 and has continued to widen since.

THE SCOPE WORTH NOTING

The NDMO framework covers fourteen domains spanning data governance, quality, metadata, master data, security, and privacy. Priority 1 is the baseline entry point, not the finish line.

Alongside these mandates, Saudi Arabia is investing heavily in AI capability across its national carriers, financial institutions, and government services. AI depends on a data foundation that has been discovered, classified, and made governable. Documentation alone cannot produce that foundation.

Riyadh Air is Saudi Arabia's new national carrier. When the airline engaged Data Sentinel, it was being built from a clean technology foundation with the ambition to satisfy NDMO across all fourteen domains, meet PDPL obligations, and support AI capability across commercial, operations, and guest experience. The brief was to build that foundation continuously, domain by domain, as documentation and operating capability come online together.

Why traditional approaches fall short.

For obligations of this shape, the standard playbook has been a policy exercise. A consulting firm scopes a maturity assessment, hands over a gap report and remediation roadmap, and cycles back at audit time. The evidence lives in binders, the controls live in policies, and the system that would actually enforce those controls sits somewhere further down the maturity curve, if it exists at all.

Two problems live inside that model.

A document is a snapshot. Between assessments, environments drift as data enters, policies age, ownership changes, and controls are followed inconsistently. By the next assessment, the binder no longer describes the environment it was written for, and the remediation work that would close that gap becomes a separate program competing for time and budget with everything else on the airline's agenda.

AI governance cannot live inside a documentation cycle. Once an AI use case is deployed against ungoverned data, the controls that should have been preventative become forensic. The question shifts from whether the risk was controlled to how large the exposure is.

Data Sentinel was engaged to build differently. The platform is being deployed inside the airline's environment, with governance authority standing up first and AI governance being built alongside the core NDMO work rather than trailing it. Data quality is monitored inside the environment as the platform matures, and evidence of enforcement is designed to flow from operation rather than from audit preparation.

The approach that works.

Three decisions early in the program have shaped how it runs today.

One. Build the operating model before the policies.

Governance authority and accountability structures went into place first, before any documentation. Decision rights, ownership, and the operating model that the Trust Layer would run on came before the artifacts they would govern. Without that authority in place, controls become suggestions and the paper trail becomes a shelf trail.

Two. Lead with one Division, then scale.

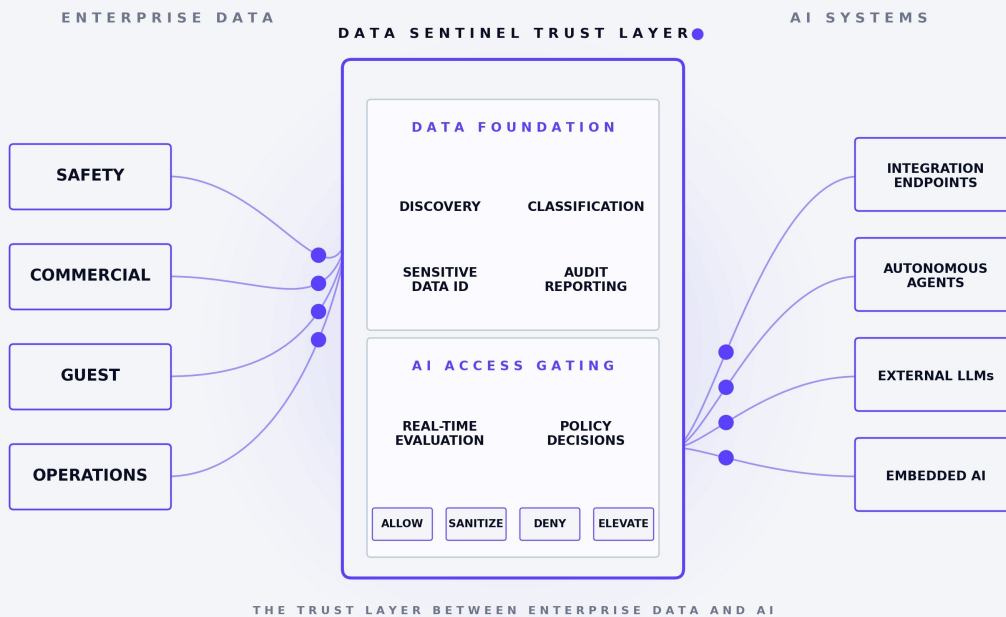
An early-adopter Division was chosen as the proving ground. Running the operating model against fourteen domains across an entire airline simultaneously would stall the program. Running it against one Division first turned the rest of the rollout into a replication exercise instead of a redesign.

Three. Stand up AI governance in parallel, not after.

The AI Governance Framework and AI Risk Management work were built alongside the core NDMO effort, not scheduled to follow it. By the time an AI use case is ready to deploy at the airline, the governance question needs to be already answered rather than freshly opened.

The Trust Layer, in practice.

The Trust Layer sits between enterprise data and the AI systems that consume it. Its Data Foundation grounds the discovery, classification, and audit reporting work already producing evidence. Its AI Access Gating layer extends that foundation into policy enforcement as the airline's AI adoption scales.



The Trust Layer between enterprise data and the AI systems that consume it.

Enterprise data flows into the Data Foundation, where it is discovered, classified for sensitivity, and reported on with audit-ready evidence. The AI Access Gating layer applies policy decisions to requests reaching out toward AI systems, with actions ranging from allow to sanitize to deny to elevate.

Four operating disciplines.

01

Governance and Operating Model

Governance authority stood up as the operating decision body for the program. Decision rights, ownership, and the operating model that every downstream control depends on.

02

AI Governance and Risk Management

A comprehensive AI Governance Framework, aligned to the EU AI Act and the NIST AI Risk Management Framework, developed and validated with stakeholders. AI Risk Management structured around the four NIST functions: govern, map, measure, manage.

03

Data Quality

Data Quality framework, standards, and rules being built inside the airline's environment. Quality monitoring running on the Data Sentinel platform. Measurable controls and continuous improvement.

04

Audit Evidence

NDMO compliance tracker updated and standardized, with deliverable formatting and evidence linkage aligned. The Trust Layer is designed to move toward compliance evidence that flows from operation rather than being assembled at audit time.

What this Trust Layer makes possible.

The Trust Layer at Riyadh Air is being built domain by domain, with governance authority in place, an AI Governance Framework aligned to international standards, and a Data Quality foundation running inside the airline's environment. What it opens up is more consequential than any single deliverable.

WHAT IT OPENS UP

- A foundation that **AI initiatives will draw from** as they scale, running against governed, quality-monitored data.
- A path toward **compliance evidence produced continuously** as operating capability matures.
- One coherent Trust Layer carrying **governance, quality, AI governance, and audit evidence** together, instead of running as separate programs.
- A foundation that supports **continued NDMO maturity progression** without re-architecture as the airline grows.

Every Data and AI Trust deliverable includes both a current-state view and a set of identified pathways that support Riyadh Air's National Data Index (NDI) maturity progression across the covered domain.

The road forward.

The program is structured to mature across three horizons, each building on what runs today.

Near-term. Depth across the fourteen NDMO domains.

NDMO maturity progression continues across all fourteen domains. As documentation lands for each domain, it feeds operational workflows for the use cases that domain governs. The Trust Layer scales through domain-level operationalization, one governed use case at a time.

Mid-term. AI governance from documentation into enforcement.

The AI Governance Framework moves from documentation into active enforcement against live AI use cases. As new AI capability is deployed at the airline, the governance question is already answered before the deployment begins.

Long-term. The Trust Layer as the airline's foundation.

The Trust Layer extends across the airline's divisions. The operating model proven on the early-adopter Division scales to the rest of the carrier as a replication exercise. The continuous foundation becomes the platform on which everything else at the airline is built.

The platform itself.

The Data Sentinel platform is on its own trajectory alongside the airline's program. The Data Foundation capabilities are in use inside the airline's environment today. The AI Access Gating capabilities are being built to sit inline on every AI-bound request. As those capabilities mature, so does the Trust Layer at Riyadh Air.

ABOUT DATA SENTINEL

Trusted data. On day one. Every day after.

Data Sentinel builds continuous Trust Layers for regulated enterprises. Our platform sits inside customer environments, classifying, governing, and producing evidence continuously.

Compliance, privacy, and AI readiness become byproducts of daily operation, not separate projects. When regulations evolve, our platform adapts. When new data enters the environment, it is classified as it lands. When auditors ask, the evidence is already there. That is what a Trust Layer does that a report cannot.

Protect

Sensitive data, continuously classified.

Comply

Evidence produced as operation runs.

Govern

Policies enforced at scale, live.

Grow

AI launched against trusted data.

HOW TRUSTWORTHY IS YOUR DATA?

*Book a demo to see
how a **continuously
operated Trust Layer**
becomes the
foundation for
compliance, quality,
and AI.*

data-sentinel.com

Data Sentinel builds continuous Trust Layers for regulated enterprises across life sciences, aviation, insurance, energy, and financial services.