SAMPLE FICTIONAL EXERCISE

This case study is a fictitious scenario constructed solely to demonstrate the author's strategic and technical approach to solving complex organizational data and compliance problems. All organizations, individuals, metrics, and events described herein are entirely fictional. No real companies, institutions, or individuals are represented.

CASE STUDY | MERIDIAN HEALTH NETWORK

Enterprise Risk Visibility Platform

Healthcare | Data Governance & Compliance Intelligence

ORGANIZATION **Meridian Health Network**

SOLUTION ARCHITECT **Manuel Munoz Jr.**

DOMAIN **Healthcare — Risk & Compliance**

VERSION **1.0**

This document presents a complete project lifecycle narrative — from initial business case and commission through architecture, implementation, and measured outcomes. It is designed to provide full transparency into how a complex compliance challenge was framed, scoped, and resolved through governed data design.

01 EXECUTIVE SUMMARY

From Fragmented Compliance to Governed Risk Intelligence

A regional healthcare system was managing compliance and risk oversight across multiple business units through a collection of independently maintained Excel files. Each unit tracked controls differently, defined evaluation criteria inconsistently, and produced reports that could not be reconciled at the enterprise level.

This engagement was chartered to replace that fragmented process with a centralized, governed risk intelligence platform — one designed not just for reporting, but for proactive risk management and audit readiness.

6	92%	100%	$310K
BUSINESS UNITS	**AUDIT PREP TIME**	**CONTROL COVERAGE**	**EST. ANNUAL SAVINGS**
Consolidated into single platform	Reduction — 22 hrs to under 2 hrs	Standardized KRI definitions	Labor + risk exposure avoided

Core Outcome

Leadership gained the ability to understand and act on compliance risks before they escalated into audit findings — replacing weeks of manual reconciliation with same-cycle visibility.

Engagement Snapshot

INDUSTRY **Healthcare**

SCOPE **Enterprise-Wide Compliance**

STACK **SQL Server · Power Query · Alteryx · Power BI**

DURATION **~6 Months**

02 BUSINESS CASE

Why This Project Was Commissioned

In Q1 of the engagement year, Meridian Health Network's Chief Compliance Officer presented the Board of Directors with findings from a third-party operational risk assessment. The assessment identified four material weaknesses in the organization's compliance monitoring infrastructure, two of which had direct exposure to CMS audit risk.

The Board authorized an internal project charter with the following stated purpose:

> **Project Charter — Stated Purpose**
> *To design and implement a centralized, governed compliance intelligence system that enables Meridian Health Network to monitor control performance in real time, reduce audit preparation burden, and establish a defensible, traceable system of record for all compliance reporting activities.*

Commissioning Drivers

!	**Regulatory Pressure**	A CMS routine audit in the prior fiscal year produced two Corrective Action Plans tied directly to the inability to produce timely, traceable compliance evidence. A repeat finding would trigger enhanced federal oversight.
$	**Cost of Manual Operations**	Internal audit estimated compliance teams were spending 18-22 analyst-hours per audit cycle on manual evidence gathering — effort that contributed zero analytical value and was entirely eliminable through automation.
?	**Leadership Confidence Gap**	Executive leadership could not answer basic risk posture questions between audit cycles. The organization was perpetually operating on compliance data that was 30-45 days out of date, with no mechanism for earlier detection.
+	**Strategic Growth Dependency**	Meridian's planned acquisition of two regional outpatient clinics required demonstrating enterprise-grade compliance maturity to the acquiring lender. The existing manual process did not meet that standard.

Project Authorization & Scope Boundaries

- Authorized budget: $480,000 (internal labor + tooling licenses)
- Timeline: 6 months from kickoff to production deployment
- In scope: All six Meridian business units — Clinical Operations, Revenue Cycle, Human Resources, Facilities, IT, and Pharmacy Compliance

- Out of scope: External reporting to regulatory bodies; EHR system modifications; legal review of control definitions
- Success criteria: Real-time compliance dashboard operational; >90% reduction in audit evidence retrieval time; standardized KRI definitions certified by Internal Audit

03 STAKEHOLDER REGISTER

Project Team & Accountable Parties

The following individuals represented the core project team and primary stakeholders across the engagement. Roles reflect both formal organizational titles and project-specific responsibilities.

NAME	TITLE	DEPARTMENT	PROJECT ROLE
Manuel Munoz Jr.	Solution Architect & Developer	External Engagement	Led end-to-end solution design, data architecture, transformation pipeline, semantic model, and reporting layer. Primary technical decision-maker throughout the engagement.
Dr. Patricia Harlow	Chief Compliance Officer	Compliance & Ethics	Executive sponsor. Defined compliance framework requirements, certified KRI definitions, and held final sign-off authority on control taxonomy.
James Whitfield	VP of Internal Audit	Internal Audit	Key governance partner. Defined auditability requirements, reviewed data lineage design, and validated that evidence traceability met external audit standards.
Renata Osei	Director, Revenue Cycle Compliance	Revenue Cycle	Business unit lead for the highest-risk compliance domain. Provided source data documentation and led control definition workshops.
Carlos Ibarra	Manager, IT Risk & Data Governance	Information Technology	Managed SQL Server environment, coordinated source system access, and oversaw RLS implementation and access provisioning.
Sandra Nguyen	Senior Compliance Analyst	Clinical Operations	Subject matter expert for clinical control evaluation criteria. Primary tester for dashboard accuracy and drillthrough validation.
Dr. Elliot Marsh	Chief Medical Officer	Executive Leadership	Executive stakeholder. Represented clinical leadership in steering committee reviews and approved clinical KRI definitions for publication.
Tanya Briscoe	Finance Director	Finance & Accounting	Ensured KRI definitions aligned with financial reporting standards and represented Finance in all metric definition workshops.
Marcus Webb	Project Manager	Enterprise PMO	Managed project timeline, stakeholder communication, and budget tracking. Served as liaison between the technical team and the executive steering committee.

04 THE REALITY OF THE PROBLEM

A System Hiding Its Own Risk

Compliance and risk management processes were fragmented across the organization in ways that made the problem self-concealing.

Each business unit maintained its own tracking mechanisms — primarily Excel-based spreadsheets with manual updates, locally defined control criteria, and no linkage between evidence files and reported metrics.

At the enterprise level, leadership faced three fundamental questions they could not reliably answer:

- Where are we most exposed right now?
- Are control failures isolated incidents or systemic patterns?
- Is our risk posture improving or compounding over time?

> **The Real Problem**
> *Audit preparation required weeks of manual effort — gathering evidence from disconnected sources, reconciling conflicting definitions, and rebuilding reports from scratch for each audit cycle. The issue was not a reporting gap. It was a trust gap.*

What Was Happening

Six business units maintained separate compliance files with incompatible structures. Metric definitions for key controls diverged without a reconciliation mechanism. By the time monthly compliance summaries were assembled, the underlying data was already stale — and no one could trace a reported number back to its source with confidence.

Where It Broke Down

Compliance reviews were reactive by design. Issues surfaced through audit findings, not through proactive monitoring. When regulators requested evidence, teams spent days locating supporting documentation that should have been centrally linked and immediately retrievable.

05 WHY THIS WAS HARD

More Than a Technical Problem

This engagement presented complexity at three levels simultaneously — data, process, and organizational alignment. Each required a different kind of intervention.

D	**Data Complexity** No standardized framework for defining or evaluating controls. Source systems operated on different update cadences with no centralized ingestion. Evidence files were stored in disconnected locations with no traceability to reported figures.
P	**Process Complexity** Manual evidence collection consumed analyst cycles that should have been focused on risk interpretation. Audit preparation was treated as a recurring project rather than a continuous capability. The organization had no baseline against which to measure improvement.
O	**Organizational Complexity** Business units had developed their own compliance workflows over years and were protective of local processes. Finance and Operations interpreted the same controls differently. Gaining alignment on metric definitions was as challenging as the technical implementation itself.
R	**Regulatory Sensitivity** Healthcare compliance data carries strict access and auditability requirements. The solution had to be defensible — not just functional. Every design decision needed to account for how it would appear in an external audit context.

Architect's Note

A senior engineer could have built a Power BI report against any one of these sources in a matter of days. The harder work — and the real value — was in designing a system that made fragmented, untrusted data safe enough to report from.

06 MY APPROACH

Alignment Before Architecture

The first instinct in engagements like this is to reach for technology. The better instinct is to ask whether the organization has agreed on what it is trying to measure — and why.

Before any modeling or pipeline work began, the project was anchored in a structured discovery phase involving compliance officers, internal audit, and operational leads from each business unit.

Discovery Objectives

- Establish a standardized definition of controls and how they should be evaluated
- Identify which metrics required strict governance versus analytical flexibility
- Map how compliance data currently flowed from source systems to reporting outputs
- Understand how decisions were being made — and where they consistently broke down
- Determine the minimum data set required to answer leadership's core risk questions

Key Design Principles Established in Discovery

Auditability over Aesthetics

Every number in the final system had to be traceable b were deferred when they conflicted with traceability.

Standardize Before Scaling

Flexible, unit-level definitions were replaced with governed enterpr required stakeholder negotiation.

Governance as a Feature

Access control, data lineage, and audit trails were desi end.

Decision Systems, Not Dashboards

The design question was always: what decision does this enable, fo what data can we show?

07 CONTROL & GOVERNANCE DESIGN

Building a System of Record, Not a Reporting Layer

The most consequential design decision in this engagement was the choice to treat the compliance platform as a governed control system rather than a dashboard on top of existing data.

This distinction shaped every downstream decision — from data model structure to access control to how KRIs were defined and calculated.

Control Taxonomy Structure

Each control in the system was formally structured across four dimensions:

Definition & Ownership
Standardized description, responsible business unit, accountable officer

Evaluation Criteria
Pass/fail thresholds, frequency, evidence requirements

Linked KRIs
Quantitative risk indicators tied to control performance over time

Evidence Traceability
Direct linkage to source records and supporting documentation

Logical Data Model (ERD)

The entity-relationship structure was designed to answer not just what controls exist, but how they have performed, where failures concentrate, and how risk evolves over time.

Dim_Control
control_key (PK) · control_name · control_category · owner_bu · evaluation_frequency

Dim_Business_Unit
bu_key (PK) · bu_name · region · compliance_officer

Dim_Date
date_key (PK) · calendar_year · fiscal_quarter · period_label

Fact_Control_Evaluations
eval_key (PK) · control_key (FK) · bu_key (FK) · date_key (FK) · evaluation_result · kri_failure_rate · evidence_ref

● FACT ● DIMENSION · FIELD

Governance Controls Implemented

- Row-Level Security (RLS): Each business unit views only its own control data within a single shared dataset
- Metric certification: All KRI definitions reviewed and signed off by Compliance and Internal Audit before deployment
- Change log: All updates to control definitions versioned and documented in the model metadata layer
- Evidence linkage: Each Fact record carries a reference key enabling direct retrieval of supporting documentation

08 ARCHITECTURE & DESIGN DECISIONS

Technology in Service of Governance

The platform was built using a layered architecture, with each component selected to enforce a specific constraint — not to maximize tooling breadth.

The guiding principle throughout: decouple data complexity from user experience. Compliance users should never have to understand the transformation logic behind a number they are reporting on.

End-to-End Architecture

SOURCE SYSTEMS EHR · Billing · HR · Compliance Databases · Manual Uploads

↓

INGESTION LAYER SQL Server Integration Services (SSIS) → Centralized Landing Zone

↓

TRANSFORMATION LAYER Alteryx Workflows → Standardized Control Evaluation Logic

↓

SEMANTIC MODEL Star Schema (Power BI Dataset) · Row-Level Security · KRI Definitions

↓

REPORTING LAYER Power BI · Executive Dashboards · Drillthrough · Subscriptions

Component Rationale

SQL Server	Centralized data store for consolidated compliance data. Chosen for transactional reliability, support for complex joins across business unit sources, and native SSIS integration for scheduled ingestion.
Power Query	Controlled ingestion and initial data shaping layer. Enabled consistent transformation rules before data entered the semantic model, reducing the risk of inconsistent pre-processing.
Alteryx	Complex transformation and standardization logic — particularly where control evaluation rules varied across units and required configurable, auditable workflows rather than embedded SQL.
Star Schema (Power BI)	Dimensional model enforcing metric consistency and query performance. Simplified consumer experience by isolating transformation logic from the reporting layer.

Row-Level Security	Implemented at the dataset level to ensure appropriate access by role. Eliminated the need for separate reports by unit — one governed dataset, filtered by identity.

09 INSIDE THE BUILD

Selected Artifacts & Design Details

The following artifacts represent key decisions made during implementation. They are included not as a tool demonstration, but to make the reasoning behind design choices fully transparent.

Artifact 1 — Transformation Pipeline (Alteryx Workflow Logic)

Control evaluation logic was implemented in Alteryx rather than embedded in SQL to support configurability across business units. Each unit's evaluation rules could be updated without redeploying the database layer.

1	**Input**	Multi-source data connector pulling from SQL landing zone by unit and period
2	**Filter**	Date range and active control filter — excludes retired or suspended controls
3	**Standardize**	Business rule application: normalize evaluation result codes to Pass / Fail / Partial
4	**Join**	Cross-reference to Dim_Control for category, owner, and threshold values
5	**Summarize**	Aggregate to control × unit × period grain for Fact load
6	**Output**	Write to Fact_Control_Evaluations staging table in SQL Server

[Visual Placeholder: Alteryx workflow screenshot — standardization and join steps]

Artifact 2 — KRI Calculation Logic (DAX)

Key Risk Indicators were implemented as certified measures in the Power BI semantic model. Centralizing calculation logic at the model layer — rather than in report visuals — ensured consistent figures regardless of where a metric was consumed.

```
KRI_Failure_Rate =
  VAR _Evaluated =
    CALCULATE(
      COUNTROWS( Fact_Control_Evaluations ),
      Fact_Control_Evaluations[evaluation_result] IN { "Pass", "Fail", "Partial" }
    )
  VAR _Failed =
    CALCULATE(
      COUNTROWS( Fact_Control_Evaluations ),
      Fact_Control_Evaluations[evaluation_result] = "Fail"
    )
RETURN
  IF( _Evaluated = 0, BLANK(), DIVIDE( _Failed, _Evaluated ) )
```

Design note: BLANK() is returned when no evaluations exist — preventing misleading zeros in sparse periods and maintaining visual accuracy on time-intelligence charts.

Artifact 3 — Star Schema (Dimensional Model Diagram)

The semantic model was organized around a central fact table representing individual control evaluations, with dimensions capturing context across controls, business units, time, and risk categories.

[Visual Placeholder: Power BI model view — star schema with Fact_Control_Evaluations at center]

> **Why Star Schema?**
> *A star schema was chosen over a normalized relational model because compliance users — not engineers — needed to interact with this data. Simplified relationships reduce filter propagation errors, improve query performance, and make the model self-documenting to a business audience.*

10 FROM DATA TO DECISION

The Reporting Experience

The reporting layer was designed around how compliance and leadership teams actually consume information — not around what the data made it easy to display.

Three distinct user personas guided the interface design:

Executive Layer

- Risk heatmap by business unit and control category
- KRI trend lines — 12-month rolling view
- Top 5 control failure categories ranked by frequency

[Visual Placeholder: Executive risk dashboard screenshot]

Operational Layer

- Drillthrough to individual control evaluations by unit
- Time-period comparison against prior quarter baseline
- Automated alerts on controls breaching threshold

[Visual Placeholder: Operational drillthrough view]

Audit Layer

A dedicated audit evidence view was implemented to support retrieval of supporting documentation directly from within Power BI. Compliance analysts could surface the evidence reference key for any control evaluation and retrieve the corresponding document from the central repository — eliminating the manual search process that had consumed significant audit preparation time.

> **The Shift**
>
> *Reactive compliance reporting → Proactive risk management. Compliance teams moved from assembling reports when asked to monitoring live dashboards and acting on leading indicators before they became audit findings.*

11 BUSINESS IMPACT

Outcomes That Changed How Risk Is Managed

The value of this engagement is best measured not in dashboard features, but in the capabilities the organization now has that it did not have before — and in the risks it can now see that were previously invisible.

The following metrics represent outcomes measured at 90 days post-deployment, based on internal audit benchmarks, analyst time-tracking, and compliance team feedback.

92%	45 days	$310K	0
AUDIT PREP REDUCTION	**LATENCY ELIMINATED**	**ESTIMATED ANNUAL SAVINGS**	**CAP REPEAT FINDINGS**
22 hrs/cycle down to under 2 hrs	Real-time vs. prior 30-45 day lag	Labor recovery + risk cost avoidance	First audit cycle post-deployment

BEFORE	AFTER
22+ analyst-hours per audit cycle spent on manual evidence gathering across 6 units	Under 2 hours per cycle — evidence directly linked and retrievable from within the dashboard
Compliance data 30-45 days out of date; no real-time monitoring capability	Same-day visibility into control performance; threshold alerts trigger within hours of a breach
Two CMS Corrective Action Plans issued in prior fiscal year; repeat risk estimated at $1.2M in fines	Zero repeat findings in first post-deployment audit cycle; CAP risk classified as resolved
Six incompatible Excel-based tracking files across business units; no enterprise rollup	Single governed compliance dataset with certified KRI definitions across all six business units
Acquisition lender flagged compliance infrastructure as a material risk to the deal	Compliance maturity demonstration satisfied lender due diligence; acquisition timeline preserved

Most Important Outcome

The organization no longer discovers compliance failures during audits. It discovers them first — through its own monitoring system — and remediates them before they become findings. That shift represents a fundamental change in risk posture, not just a reporting improvement.

12 TRADE-OFFS & LESSONS

What Was Optimized, What Would Be Refined

Every architectural decision involves trade-offs. Naming them explicitly — rather than presenting the solution as optimal — is more honest and more instructive.

DECISION POINT	CHOSEN APPROACH	RATIONALE
Transformation layer location	Alteryx (external workflow)	Prioritized delivery speed and business unit configurability over architectural elegance. A production-scale version would consolidate more logic into the SQL layer for maintainability.
Control definition governance	Strict standardization	Chose governance over flexibility. Some units lost the ability to track non-standard metrics. This was the right trade-off — but required active stakeholder management.
Model complexity	Simplified star schema	Chose query performance and user interpretability over analytical flexibility. More complex analyses require downstream measures, not ad-hoc model exploration.
Report layer scope	Three fixed persona views	Resisted the temptation to build a fully self-service model. Fixed, certified views are more defensible in an audit context than open-ended exploration.

What I Would Refine in a Next Version

- Move all control evaluation logic into SQL stored procedures, with Alteryx serving only as an orchestration layer — not a transformation engine
- Implement a formal data lineage catalog to track field-level transformations across the full pipeline, not just at the semantic model level
- Introduce an automated KRI threshold review cycle — current thresholds were set at implementation and require manual governance to stay calibrated
- Build a dedicated audit package export view that assembles evidence references into a structured PDF package for external reviewer consumption

Key Principle Reinforced

In regulated environments, a well-designed compliance system is not just technically correct — it must reduce ambiguity, not introduce it. Every design decision should be explainable to an auditor, not just to a data engineer.

13 KEY TAKEAWAY

Confidence in Compliance Posture

This engagement was ultimately about establishing a trusted, governed system for managing compliance and risk — not about building a more sophisticated spreadsheet replacement.

The technology was secondary. The primary work was in defining what needed to be true about the data before any of it could be trusted.

> *"A compliance platform that cannot explain its own numbers is not a governance system.*
>
> *It is a more sophisticated way to be wrong."*
>
> — Manuel Munoz Jr.

This Case Study Demonstrates

- Problem framing before solution design — alignment was treated as a prerequisite, not a courtesy
- Control system thinking — the platform was designed for auditability, not just usability
- Architecture grounded in governance constraints — every technology decision was justified against a specific design principle
- Senior-level trade-off transparency — what was optimized, what was deferred, and what would be improved in a production scale version