GRC Platform Implementation

Tier-1 Global Bank — MetricStream Deployment

From Fragmented Spreadsheets to an Integrated Risk Platform

At a Glance

Organisation	Tier-1 Global Bank (anonymised)
GRC Platform	MetricStream
Implementation Scope	Enterprise-wide, all risk & compliance functions
Timeline	12–18 months (typical for banking sector)
Approach	Phased rollout across 5 structured lifecycle stages
Starting Point	Fragmented spreadsheets; inconsistent risk definitions
End State	Integrated platform with continuous control monitoring

Background & Challenge

Large financial institutions routinely rely on Governance, Risk & Compliance (GRC) platforms to consolidate risk management across geographies and business units. Before deployment, most banks operate with siloed, spreadsheet-driven processes that create significant gaps in visibility, consistency, and control.

This Tier-1 global bank faced three core challenges prior to adopting MetricStream:

- **Fragmented spreadsheets** spread across departments, with no single source of truth.
- **Inconsistent risk language —** different units applied different definitions to the same categories. “High Impact” meant a $1M loss in one department and reputational damage in another.
- **No real-time visibility,** relying on annual audits rather than continuous monitoring.

Implementation Lifecycle: Five-Stage Approach

The bank’s transition followed a rigorous five-phase lifecycle. Each phase built directly on the last, ensuring foundational decisions around taxonomy and data ownership held firm throughout the technical build and go-live.

Phase 1 Diagnostic & Taxonomy Alignment (Analysis)

Before any configuration began, the bank resolved its fundamental "language problem" — ensuring all stakeholders worked from a shared set of definitions.

Gap Analysis

Auditors conducted a cross-departmental review and uncovered significant definitional inconsistencies:

- **Credit Risk** defined "High Impact" as a financial loss exceeding $1 million.
- **Operational Risk** defined the same term by reputational damage, with no dollar threshold.

Standardisation: Common Risk & Control Library (RCL)

The bank created an agreed-upon catalogue of 500+ standard controls, including Monthly Reconciliations and User Access Reviews. Every department committed to the same definitions before technical work began.

"Golden Source" Identification

Each data domain was assigned a single authoritative source system:

- **HR System** → recognised source for employee lists.
- **Core Banking System** → authoritative source for transaction volumes.

Phase 2 Functional Design & Prototyping

Rather than a risky "Big Bang" rollout, the team designed and deployed in modules, prioritising high-visibility outputs first.

Module Prioritisation

Enterprise Risk Management (ERM) was selected as the first module because it produced the Board-level Risk Heatmap — providing immediate, visible value to senior leadership.

Workflow Mapping: The "Life of a Finding"

The end-to-end workflow for raising and resolving an audit finding was mapped across four steps:

1. Auditor logs the issue in the system.
2. System automatically notifies the relevant Business Owner.
3. Business Owner submits a formal remediation plan.
4. System tracks the plan to its Target Date; if missed, the Chief Risk Officer (CRO) is automatically alerted.

Phase 3 Technical Build & Integration

With design approved, the technical team connected MetricStream into the bank's existing infrastructure.

API Integration

- **Internal Audit systems** — for seamless issue ingestion and tracking.
- **External Regulatory feeds** — to keep control requirements current with evolving compliance obligations.

Role-Based Access Control (RBAC)

Strict "need-to-know" access rules were configured. A team member in the UK branch was unable to view risk assessments from the Singapore branch unless explicitly authorised.

Offline Briefcase Mode

For auditors in remote branches with unreliable connectivity, an Offline Mode was configured: findings could be logged locally and synchronised with the central platform upon reconnection.

Phase 4 Pilot & User Acceptance Testing (UAT)

Wealth Management was selected as the controlled pilot environment before organisation-wide rollout.

Parallel Run (3 Months)

The Wealth Management team ran both systems simultaneously — completing risk assessments in legacy spreadsheets and in MetricStream in parallel — to validate that outputs were consistent.

The "Friction" Test

User experience was quantitatively measured. A manager should complete a Control Self-Assessment (CSA) in under 15 minutes. Any interface exceeding this threshold was redesigned before broader rollout.

Phase 5 Go-Live & Cultural Embedment

The final phase focused on making risk management a genuine part of daily working culture, not just a compliance checkbox.

The "Carrot and Stick"

Leadership formally tied Risk Performance — as tracked within MetricStream — to departmental bonus KPIs. This single decision drove adoption at all levels of the organisation.

Continuous Control Monitoring (CCM)

The bank moved away from its legacy annual audit cycle. MetricStream now ingests control data daily. If a control fails, the relevant team is notified within 24 hours — compared to the previous model where the same failure might go undetected for up to 12 months.

Key Outcomes & Lessons Learned

Critical Success Factors

- **Taxonomy first:** standardising definitions before build prevented costly rework.
- **Modular rollout:** prioritising the Board Heatmap created early momentum and executive buy-in.
- **Controlled pilot:** the parallel run caught discrepancies early in a low-risk environment.
- **Incentive alignment:** linking the GRC tool to bonus KPIs ensured genuine cultural adoption.

Lessons & Risks to Watch

- **The "language problem"** is almost always underestimated. Allow significant time for taxonomy alignment before any technical work begins.
- **Change management** is as important as technical configuration. Without cultural embedment, platform adoption typically fails.
- **A parallel run,** while resource-intensive, is essential validation. Skipping it introduces unacceptable UAT risk.

Conclusion

This case study demonstrates that a successful GRC platform implementation is far more than a technology project. It is a governance transformation — one that requires equal rigour in data standards, workflow design, change management, and leadership commitment.

The five-stage lifecycle applied by this Tier-1 bank provides a replicable framework for any financial institution seeking to move from fragmented, reactive risk management to an integrated, continuous-monitoring model. The fundamental shift — from detecting control failures twelve months after the fact to detecting them within twenty-four hours — represents a step change in the institution's risk posture.