Technology Strategy for Your GRC Journey

Vinay Bapna
Vice President – Marketing
MetricStream

Are You Seeing the Change?
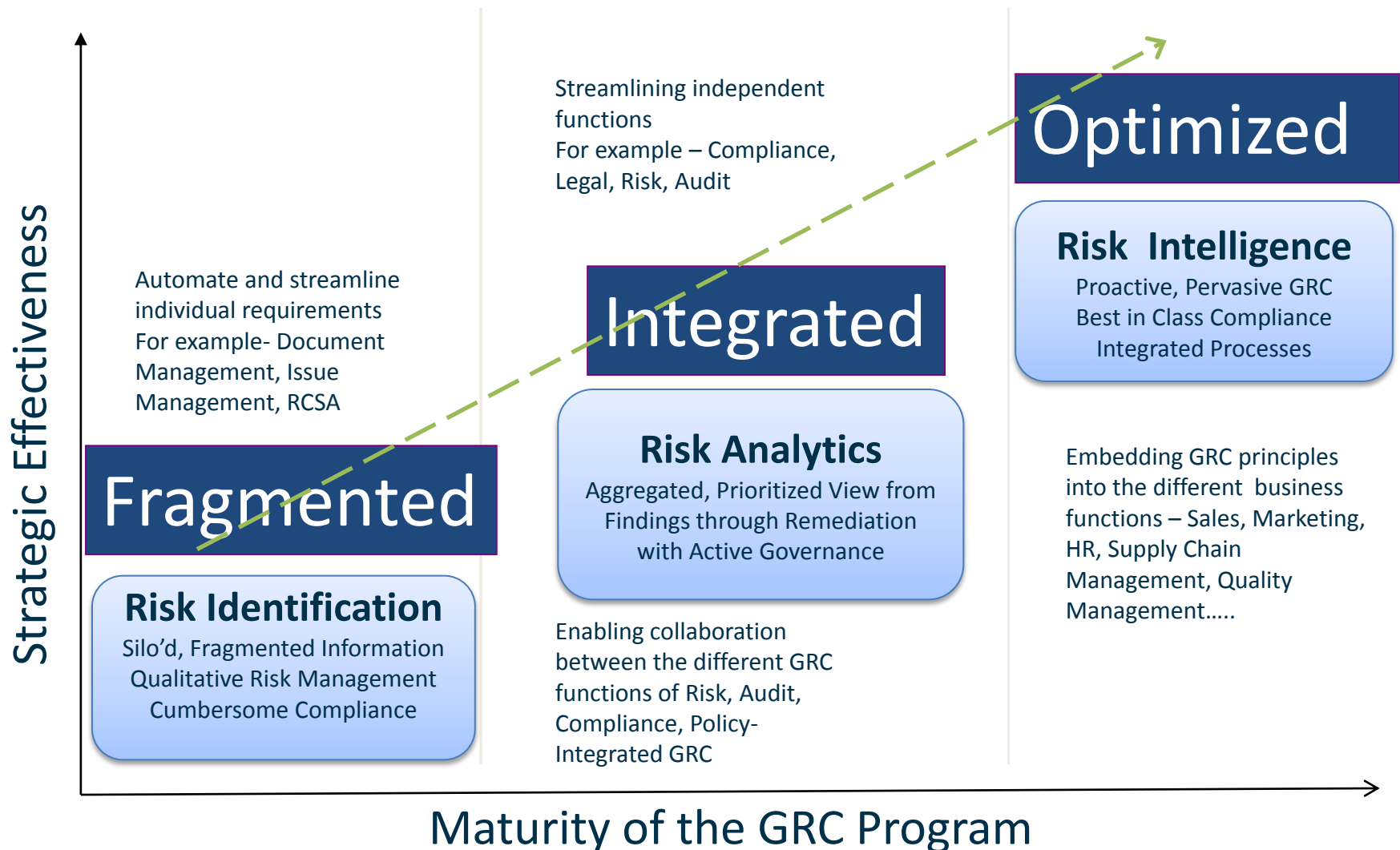
1. Performance Focus

2. Regulatory Changes

3. Cloud, Social Media, Mobile

4. Complex Global Vendor Ecosystem

5. Proliferation of Requirements

How are you changing?

GRC Journey

Strategic Effectiveness ↑

Optimized

Risk Intelligence
Proactive, Pervasive GRC
Best in Class Compliance
Integrated Processes

Streamlining independent functions
For example – Compliance, Legal, Risk, Audit

Integrated

Automate and streamline individual requirements
For example- Document Management, Issue Management, RCSA

Risk Analytics
Aggregated, Prioritized View from Findings through Remediation with Active Governance

Embedding GRC principles into the different business functions – Sales, Marketing, HR, Supply Chain Management, Quality Management.....

Fragmented

Risk Identification
Silo'd, Fragmented Information
Qualitative Risk Management
Cumbersome Compliance

Enabling collaboration between the different GRC functions of Risk, Audit, Compliance, Policy- Integrated GRC

Maturity of the GRC Program →

Pervasive GRC

- ## Embedded in day to day Business, IT, Security processes
  - Proactive vs Reactive
  - Driving performance vs post-facto assurance
  - Examples: Policy

- ## Anytime, Anywhere
  - Web, Offline, Mobile, Cloud access

- ## Contextual coverage of 'Core' and 'Long-tail'
  - Information aggregation from multiple systems and sources
  - Apps that span a wide spectrum of use cases,
  - Leverages a federated taxonomy and contextual insights for decisioning

What is GRC Journey?

GRC Journey is about deriving value from GRC investments, helping accelerate organizational readiness to successfully implement a diverse and valuable set of use cases on the journey towards Pervasive GRC

Why GRC Journey?

Recognize that GRC Program implementation is a Journey

It begins with consolidating efforts around priority initiatives such as policy management, risk management, privacy, security or corporate compliance and grows to embrace new stakeholders and use cases

Manage GRC as a program, involving people, processes and technologies

Phased, multi-month or multi- year initiatives that will allow your organization to realize immediate value, while building a solid GRC foundation that will support long-term goals.

GRC Journey – Addressing Key Challenges

GRC Maturity and Deriving Value from GRC Investments
Focus on right priorities to achieve better performance, make better decisions

GRC Journey Planning
Build a clear program with key stakeholders

GRC Platform, Data Model for Federation
Build Federated taxonomies across different business units

GRC Applications with Accelerated Deployments
Streamline and automate for high value

Continuous Improvement
Engage in our Community for Innovation and Change

Federated Architecture

- ## Enables Agility, Flexibility

  - Supports Different Taxonomies
  - **Horizontally** across GRC groups - SOX, Audit, Risk, Vendor, IT, Legal
  - **Vertically** across business groups - Corporate, BUs, Country, Product Line, Division, Subsidiaries
  - Centralized control, decentralized ownership
  - Multi-dimensional relationships with roll-up reporting
  - Multiple groups can use the same artifacts while having variants

MetricStream

Welcome: **Program Manager**

My Tasks: 14 [7 New, 0 Past due]

Compliance | **Administration**

Assignments | Dashboards | Reports

Browse: Processes

- Affirmative Action Plans
- Branch Admin
- Certifications in Connection w
- Certifications in Connection w
- Citations
- Commercial Banking Group
- Commercial Lending
- Conduct FERC Training
- Conduct FERC Training by sunde
- Construction Lending Manual
- Consumer Lending
- Consumer Lending Support
- Corporate Security
- Credit Administration
- Credit Card Services
- Dealer Banking
- Deposit Operations
- Distributed Capture
- Electronic Funds Transfer
- Employee Banking
- Examinations and Inspections
- Exclusion for News Media
- Home Loan Division
- INTERVEST
- ISS / Grant Program Management
- Information Technology
- Item Processing
- Loan Servicing
- Marketing

Done

Process: Electronic Funds Transfer [PROC-1055]

Linkages between Regulations, Policies, Requirements, Risks, Controls, Organizations, etc.

Processes

Processes Mapped to Risks

MetricStream

Welcome: **Program**

Compliance | **Administration**

Assignments | Dashboards | Reports

Browse: Processes

- Electronic Funds Transfer
  - Process
    - All Processes - General
      - Risk
        - Identify theft
        - EFT Related frauds
        - Unauthorised transactions
        - Non compliance with Regulatory
        - Reg E related Automation tools
        - Reputation risk due to delays
        - Customer account statements do
  - ACH
  - Mobile Banking Transactions
  - ATM Banking
    - Risk
      - ATM Frauds
      - Poor customer service
      - Forged notes
      - Short cash dispensed
  - Overdrafts
    - Risk
      - Charing overdraft fees without
      - Overdraft Protection program n
      - Misleading marketing and opt i
      - Inadequate disclsoure of opt i
  - Net banking Transfers
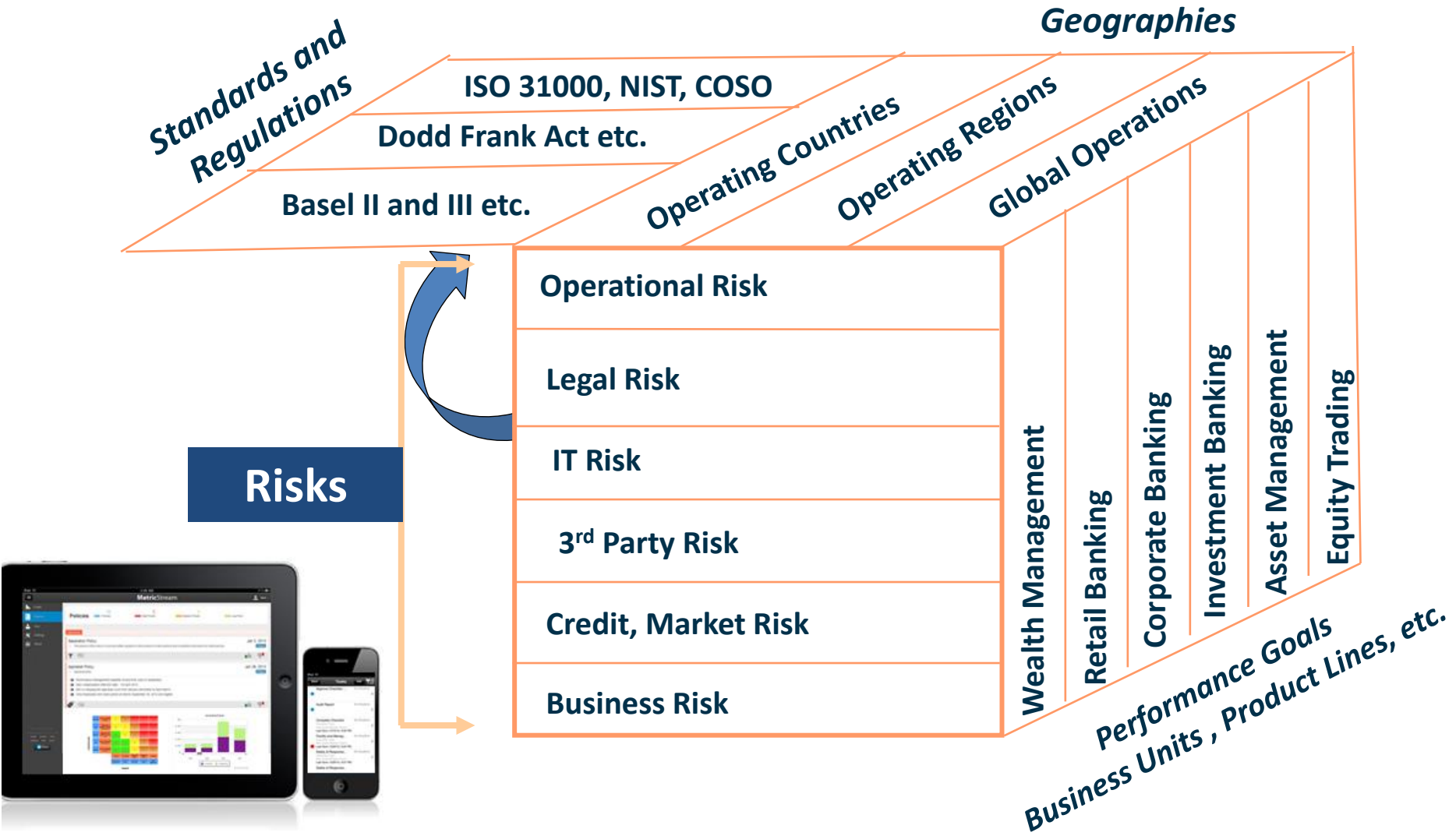   - Risk
      - Fraudulent transfers over Net

MetricStream

Compliance | Administration

Create/Manage | Reports/Dashboards

Browse: Regulatory Bodies

- DOL
- EEOC
- FDIC
  - Area of Compliance
    - Policy AYU29822
      - FDIC
      - Model Reference
        - Portion 1
        - Citation 2
        - Portion 2
        - Section 1
        - Citation 1
    - Regulation E
      - FDIC
      - Requirements
        - Portions
        - Citations
        - Sections
- HHS

Modeling Organizational Structures and Hierarchies

Geographies

Standards and Regulations

ISO 31000, NIST, COSO

Dodd Frank Act etc.

Basel II and III etc.

Operating Countries

Operating Regions

Global Operations

Risks

- Operational Risk
- Legal Risk
- IT Risk
- 3rd Party Risk
- Credit, Market Risk
- Business Risk

Wealth Management

Retail Banking

Corporate Banking

Investment Banking

Asset Management

Equity Trading

Performance Goals

Business Units , Product Lines, etc.

Case Study – Large Consumer Product Brand

Challenges

- Highly regulated product mix (Global/Local)
- Visibility into risks across multiple business units and suppliers
- Alignment of policies and procedures across 200,000+ employees and suppliers

How MetricStream Helped?

- Common platform for rationalizing risk and control framework
- Federated data model to support multiple business units
- Reduce cost with common issue management processes

Business Benefits

- Streamlined processes for better compliance
- Lowered risks with higher visibility
- Better governance across business units and supplier networks
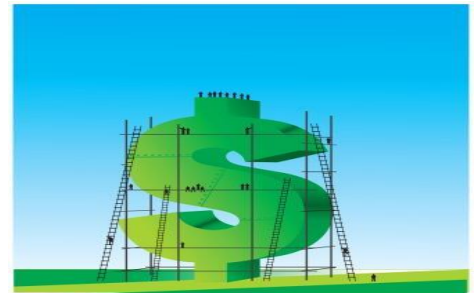
Collaboration Across GRC Functions

- Tracking Regulatory Changes
- Implementing and Assessing Controls
- Program Tracking

Compliance Management

- Email Integration
- Document Interoperability

- Federated Compliance Reporting

Risk Management

Compliance Risk

Regulatory Violations

Policy Mgmt.

Issues Management/ Remediation

Dashboards & Reporting

- Assessing Risk related to Non-Compliance
- Risk Assessment
- Quantitative and Qualitative Analysis

Auditable Entities

Identified Gaps

- Closed Loop Issues Management

Audit Management

- Work Program Library
- Electronic Workpapers
- Scheduling
- Remediation
- Reporting
- Resource Management

- Other Compliance Reporting

Configurability: Ensure Long-term Success

- Map pre-packaged solutions to your business processes
  - Easy user adoption
  - Organizational change management

- Adapt to changing business requirements
  - No vendor dependency
  - Change control

- Minimize support and maintenance overheads
  - Costs, Staffing
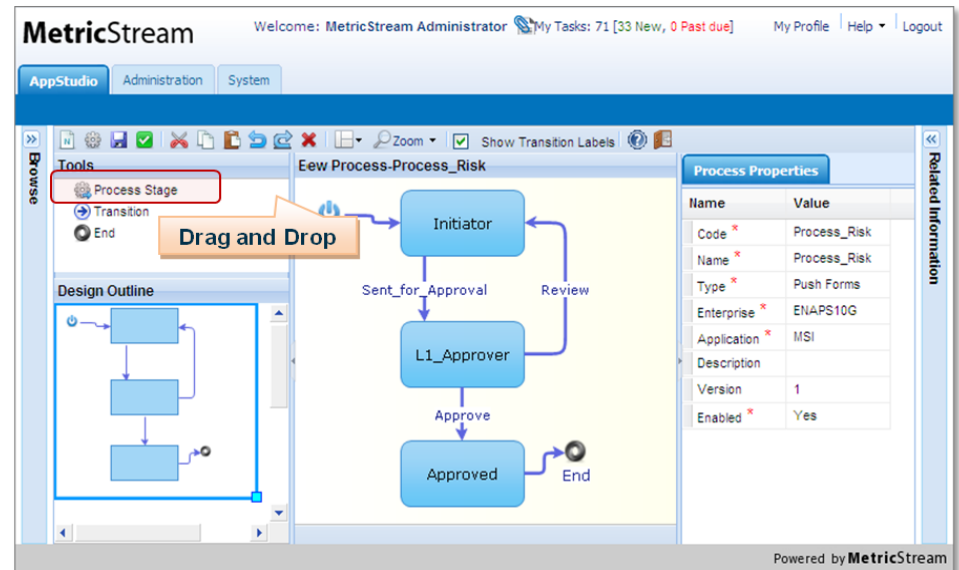
Compliance Content and Regulatory Changes

- Policy and compliance activities

- Impact analysis and mapping

- Triggering assessments, policy updates

Case Study – Diversified Financial Services Company

Challenges

- Timely respond to high number of regulations
- Risk, compliance and supplier management processes
- Consistent and insightful reporting for board and executives

How MetricStream Helped?

- Regulatory intelligence with curated content
- Comprehensive audit and compliance management initiative
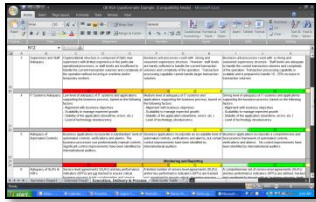- Common platform for rationalizing risk and control framework

Business Benefits

- Streamlined process and impact analysis with regulatory process change
- Efficiencies gained through risk analysis and reporting
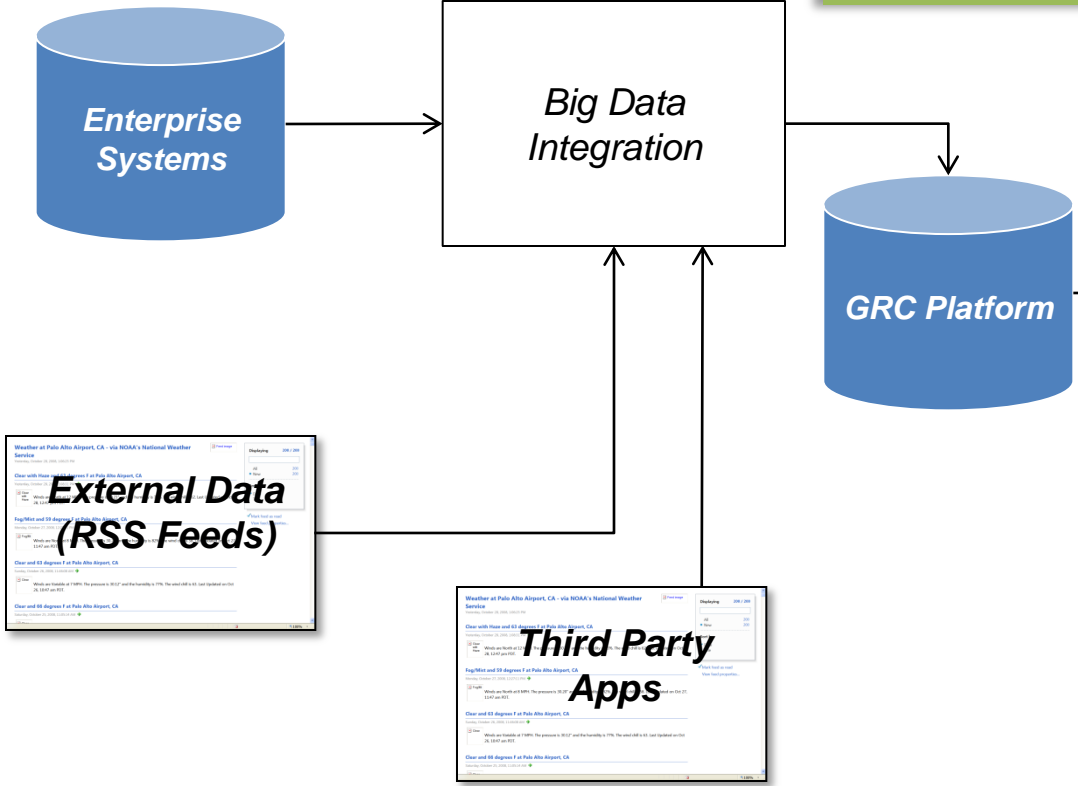- Agile responsiveness to change and better governance

Integration: GRC as Infrastructure

- Aggregation of structured and unstructured data (Big Data)
- Analytics for risk intelligence and contextual analysis
- Orchestration of native & non-native apps

Enterprise Systems → **Big Data Integration** → **GRC Platform**

External Data (RSS Feeds)

Third Party Apps

KRI Dashboard

Social Media Risk Analysis

GRC Implementation Performance Excellence

- **Faster Time-to-Value**
  - Artifacts for accelerated deployment
  - Methodology, planning tools, libraries, configuration workbooks

- **Agile Iterative Approach**
  - Enable taxonomy harmonization, on ramping, change management, IT alignment

- **Domain Expertise**
  - Experienced GRC professionals to align the solutions as well as provide advice on improving those programs

How Technology Enables GRC Journey

- ## Federation & Collaboration
  Ensure flexibility and extensibility

- ## Configurability & Agility
  Map to existing and changing business processes

- ## Integration
  Interface with external systems and data sources

- ## Content
  Leverage content sources seamlessly

- ## Implementation
  Focus on time-to-value drivers

"Every journey starts with a single step."
– Confucius

Thank You