Navigating Your GRC Journey

Orchestrating Pervasive GRC, GRC Technology and Process Implementation Considerations

Dr. Brenda Boulwood
Senior Vice President, Industry Solutions,
MetricStream
Pervasive GRC - Change Drivers

Yesterday’s World

- Proliferation of GRC
- Changing Regulatory Landscape
- Management Oversight
- Convergence of Business
- Creating a Single View

Required

INTEGRATED GRC

- Single Source of truth
- Integrated Functions
- Breaking of Information Silos
- Collaborative Workflows

Today’s World

- Hyper-Connectivity
- Social Media
- Globalization
- Mobility
- Virtualization

Required

PERVERSIVE GRC

- Single source of truth but different visibility for different perspectives
- All encompassing processes involving all organizational functions
- Ability to achieve different objectives for different groups with a common framework
- Embedded non-intrusively in the daily workings of the organization

Third Generation

Navigating Your GRC Journey

Fourth Generation
Pervasive GRC - Implications

- Enterprise Wide GRC Culture
- Involvement of All Function Lines
- Ease of Participation driving adoption
- Creating a Common Taxonomy

Pervasive GRC Achieves Different Objectives for Different Groups but with a Common Framework

- Inclusive processes traversing multiple functions
- Processes beyond IT infrastructure boundaries
- Uniform process definitions across BUs
- Uniform process across geographic units

- Developing an integrated data infrastructure
- Non intrusive tools and enablers
- Multiple access points and support for multiple interfaces
Orchestrating Pervasive GRC

1. GRC Adoption
   - Used by a modern and diverse user base

2. GRC Layering
   - Embedded within a modern Enterprise Architecture

3. GRC Contextualization
   - Adapted to the context of modern Enterprises
GRC Adoption - Objectives and Framework

Vision

A system of engagement for Generation C users

Framework

• Bidirectional Interaction - Building a User Friendly Interface
• Contextual Information - Providing context to information
• Ubiquitous Touch Points - Multiple devices and form factors
• Behavioural Construct - Social networking related interactions
• Immersive Experience – Using Gamification

Key Objectives

• Inclusive GRC Programs involving Business, IT and GRC Functions
• Non Intrusive GRC Programs working seamlessly woven into the organizational fabric
• Enablement of Business Functions to achieve business objectives
Adapted to the dynamic context of a modern organization

**Vision**

**Framework**

- **Federated data models** building context to information
- **Apps for Contextual Requirements** to adapt and develop GRC applications for the organization’s specific needs
- **Contextual Information** through GRC Intelligence for content and intelligence at context and within the platform
- **An App for each need** through Zaplet to create a marketplace for long-tail GRC applications

**Key Objectives**

- **Contextual Information** for each person, each unit and each region within the organization
- **Contextual Apps** for each requirement, each functionality, each feature and each content
- **Contextual Visibility** providing the right perspective to the relevant situation
GRC Layering - Objectives and Framework

Vision

Part of the fabric of a modern Enterprise’s landscape

Framework

- **Predictive and Prescriptive Risk Analytics** through Reporting, and Diagnostic across multiple business, IT, security functions
- **Bidirectional linkage** with business process systems
- **Cloud Architectures to support** Open APIs for continual extension
- **Big data analytics** on next gen scale and complexity

Key Objectives

- **Single Source of Truth with multiple perspectives** built into the pervasive GRC program
- **One Framework but different objectives** for different groups interacting
- **Aggregation of relevant information** into a single system

Navigating Your GRC Journey
Orchestrate the People

- Reputational Risk
- Human Capital Risk
- Process Related Risk
- Legal Risk
- Approval
- Create eCheck
- Capture
- Create PO
- Vendor
- Receive Payment & Remittance Advice
- Store Centrally
- Finance
- Risk
- Compliance
- Audit
- External Audit
- Third Party/Vendor Risk
- Geo-political Risk
- BCM Risk
- Technology / Security Risk
- Executive Management
- Departments

- Develop a collaborative relationship between all stakeholders
- Develop strong executive management support for a best in class risk & control framework
Orchestrating the Data

From Data to Insight
Orchestrate the Common Taxonomy

- Many to Many Relationships between multiple GRC Data Objects
- GRC data objects stored in structured libraries with ease of access
- Reduced redundancy and improved accountability due to defined relationships

MetricStream GRC FUNDATION

AppStudio
- Forms
- Data
- Workflow
- Data Import
- Templates

GRC Foundation
- Objectives
- Risks
- Controls
- Processes
- Assets
- Organizations
- Regulations

Infrastructure
- Web Portal
- Mobile API
- Reports
- Analytics
- Infolets
- Security
- Alerts
- Offline Briefcase

Unstructured Data
Relational DB
Big Data
Architected for Pervasive GRC

Horizontal Solutions
- (VRM, ORM, Internal Audits, IT GRC, QMS, etc.)

Vertical Solutions
- (Financial, Healthcare, Energy & Utilities, etc)

MetricStream Apps
- Risk Mgmt
- Compliance Mgmt
- Audits Mgmt
- Survey Mgmt
- Loss Mgmt
- Threats & Vulns.
- Supplier Onboarding
- Issue Mgmt

[+] other Apps

Zaplet Appstore
- 3rd-Party Apps
- Community

GRC Intelligence
- Content
- Alerts & Feeds
- Community

Compliance Online
- Training
- Retail Content

AppStudio
- Forms
- Data
- Workflow
- Data Import
- Templates

GRC Foundation
- Objectives
- Risks
- Controls
- Processes
- Assets
- Organizations
- Regulations

Infrastructure
- Web Portal
- Mobile API
- Reports
- Analytics
- Infolets
- Security
- Alerts
- Offline Briefcase

Unstructured Data
Relational DB
Big Data
GRC Journey - Time to Value

- **Fragmented**
  - Risk Identification
    - Silo’d, Fragmented Information
    - Qualitative Risk Management
    - Cumbersome Compliance
  - Automate and streamline individual requirements
    - For example - Document Management, Issue Management, RCSA

- **Managed - Integrated**
  - Risk Analytics
    - Aggregated, Prioritized View from Findings through Remediation with Active Governance
  - Enabling collaboration between the different GRC functions of Risk, Audit, Compliance, Policy-Integrated GRC

- **Optimized**
  - Risk Intelligence
    - Proactive, Pervasive GRC
    - Best in Class Compliance
    - Integrated Processes
  - Embedding GRC principles into the different business functions – Sales, Marketing, HR, Supply Chain Management, Quality Management.....

- **Maturity of the GRC Program**
  - Streamlining independent functions
    - For example – Compliance, Legal, Risk, Audit

**Navigating Your GRC Journey**
GRC Journey - 5 Key Challenges & How MetricStream Helps

• **GRC Maturity and Time to Value – Focusing on the right priorities to achieve Better Performance, Better Decisions**
  - Maturity Model of GRC processes - quick wins and building the foundation

• **GRC Journey Planning – Building a clear program with key stakeholders**
  - GRC Journey Guidebook for Champions - Vision and Governance model, Stakeholder Mapping, GRC Program Strategy, Design and Implementation blueprint

• **GRC Platform, Data Model for Federation – Building Federated taxonomies across different business units**
  - GRC Foundation - core content on example org models, risks, controls and access control models, with taxonomies supporting distinct units

• **GRC Applications with Accelerated Deployments – streamline and automate for high value**
  - MetricStream Application Configuration Workbooks - streamlined process, best practice, accelerated time to value with base application

• **Continuous Improvement – Community for Innovation and Change**
  - MetricStream GRC Journey Special Interest Groups - community of peers sharing what works, GRC program plans/artifacts and successes!
GRC Journey - Example

MetricStream Applications and Workstreams

MetricStream Platform and GRC Foundation
Risk and Control Framework, Risk Reporting, Analytics and Governance
GRC Organization Hierarchy, Asset Integration

Audit Management
SOX Compliance Management
Global Reg Compliance
IT Risk Management
Risk and Control Library
Training and certifications
OpRisk
Issue Management

Inflotet Integrations: Data feeds

MetricStream Deployment Methodology for Each Workstream

Discovery Requirements Workshop
Design, Develop, Configure, and Test
User Acceptance Test Environment Set Up
Training and User Acceptance Testing
Production Deployment

Navigating Your GRC Journey
GRC Journey - Key Benefits

• **MAKE BETTER DECISIONS, LOWER RISKS**: Manage its most urgent business risks across the silos of finance, legal, compliance, operations and IT/Security
  
  **Key Benefit**: Reduce Risk by gaining visibility and context

• **IMPROVE PERFORMANCE AND GAIN EFFICIENCIES**: Collaborate, through a federated governance model, with other major programs in place or being implementing – bringing all the key stakeholders together through a common risk and control framework
  
  **Key Benefit**: Gain efficiencies and lower costs by streamlining processes and leveraging a consistent risk and control framework, collaboration and overall methodology

• **OPTIMIZE REPORTING and GOVERNANCE**: Report the right information to the right people, at the right time
  
  **Key Benefit**: Clear understanding of the information and analytics required for the Board, Regulators, Leadership, External and Internal stakeholders
## Overcome the Barriers

<table>
<thead>
<tr>
<th>Barrier</th>
<th>How to Overcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Quality</td>
<td>Agree the golden source for each type of data and add workflow approval steps</td>
</tr>
<tr>
<td>Taxonomy</td>
<td>Allow tiers in the data models to allow aggregation while local language can be used by businesses and functions</td>
</tr>
<tr>
<td>Too Complex</td>
<td>Start small, and execute towards a common vision</td>
</tr>
<tr>
<td>Culture</td>
<td>Collaborative leadership to overcome the information and organizational silos</td>
</tr>
</tbody>
</table>