GRC Fundamentals

Vinay Bapna, Associate Vice President - Marketing
GRC in Today’s World

• Performance Focus
  – Risk intelligence has to drive performance in a growing enterprise

• Regulatory Changes
  – Significant business and cost impact on corporations

• Cloud, Social Media, Mobile
  – Emerging risks from faster, unrestricted, information flows

• Complex Global Supply Chain
  – Intertwining of risks and escalation of incidents
The GRC Journey: Levels of Maturity

Maturity of the GRC Program

- **Fragmented**
  - Streamlining independent functions
  - For example – Compliance, Legal, Risk, Audit

- **Managed**
  - Automate and streamline individual requirements
  - For example – Document Management, Issue Management

- **Integrated**
  - Enabling collaboration between the different GRC functions
  - - Integrated GRC

- **Optimized**
  - Embedding GRC principles into the different business functions
  - - Sales, Marketing, HR etc
Enabling a Common GRC Taxonomy

Defining a common GRC taxonomy that provides a baseline across the organization as well as a federated model that allows aggregation and roll-ups.
Data Model: Flexible Relationships and Visualizations

Processes

Processes Mapped to Risks

Linkages between Regulations, Policies, Requirements, Risks, Controls, Organizations, etc.
Case Study: Robust Compliance Data Model

Leading Retail Chain

• Streamlining and integrating compliance programs across BUs and functions

• Integrated framework to streamline compliance with HR policies and procedures, training and certification requirements, privacy policies, diversity affairs, legal requirements, risk management, internal audit, IT security and SOX
Defining hierarchies and relationships for a centralized view of risk aligned to business performance objectives for enabling decision making

Operational Risk

Legal Risk

IT Risk

3rd Party Risk

Credit, Market Risk

Business Risk

Standards and Regulations

ISO 31000, NIST, COSO

Dodd Frank Act etc.

Basel II and III etc.

Geographies

Operating Countries

Operating Regions

Global Operations

Performance Goals

Wealth Management

Retail Banking

Corporate Banking

Investment Banking

Asset Management

Equity Trading

Business Units, Product Lines, etc.
GRC and the Organization's DNA

- **Federated architecture**
  - Centralized controls and visibility
  - Decentralized processes and ownership
  - Supporting complex, multi-dimensional relationships

- **Large scale adoption**
  - Extended enterprise participation
  - Simplified user experience
  - Collaboration, personalization, mobile access
Case Study: Federated GRC Infrastructure

A Fortune 50 Life Sciences Company

• Federated GRC framework across 400 business units

• Regulatory, Operational and IT compliance - driven by the board

• Harmonization of controls across the enterprise and subsidiaries

• Finance, IT, privacy, security, marketing, sales, safety, environment and quality
Monitoring Regulatory Changes

- Update policy and compliance activities
- Impact analysis and mapping
- Triggering assessments, policy updates
Case Study: Regulatory Monitoring

One of the Largest Banks in Europe

• Streamlined and simplified compliance by integrating risk assessments across countries, functions and processes

• Comprehensively assess and manage risks, establish and monitor controls and meet the demands of regulations across 80 countries

• Integration with external regulatory sources for risk intelligence
Channel: NYSE Feed

Channel Name*: NYSE Feed
Channel Status*: Active

Channel Type*: Alert

Source Details

Delete Add Source Delete Last Source

Row# 1

Source*: RSS
Server Address / URL*: http://markets.nyx.com/content/msa_traderupdates/all/

User Name: Kris
Password: ********

Server Parameter(s)

Keyword(s) (Comma Separated)

Validate Source
Enabling Collaboration Across GRC Functions

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

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

- Issues Management/Remediation

- Closed Loop Issues Management
- Work Program Library
- Electronic Workpapers
- Scheduling
- Remediation
- Reporting
- Resource Management

- Federated Compliance Reporting
- Closed Loop Issues Management
- Other Compliance Reporting

- Email Integration
- Document Interoperability

- Compliance Management

- Policy Mgmt.

- Risk Management

- Audit Management

- Dashboards & Reporting

- Other Compliance Reporting

- Federated Compliance Reporting

- Compliance Risk

- Identifiable Gaps

- Auditable Entities

- Regulatory Violations

- Compliance

© 2013 MetricStream, Inc. All Rights Reserved.
Enabling Collaboration: Calendar, Emails, Workflows

Compliance Survey Collaboration
Next Gen GRC Platform Capabilities

• Big Data Analytic Capabilities

• Contextual Risk Intelligence and Advanced Analytics

• Advanced AppStudio for Configuration

• Multi-platform Mobility Support

• Cloud-based Solution

• Readiness for Enterprise
Social Media Risk and Compliance Management
Leveraging Native Mobile Capabilities
LHR-1 Anti-discrimination

1.1 Equal Opportunity

Suppliers shall not discriminate against any worker based on race, color, age, gender, sexual orientation, ethnicity, disability, religion, political affiliation, union membership, national origin, or marital status in hiring and employment practices such as applications for employment, promotions, rewards, access to training, job assignments, wages, benefits, discipline, and termination.

Suggested Documents

Bacon ipsum, dolor sit amet, ut et dui, meatball commodo ham salami, labore bacon, officia id excepteur, Velit doner meatball, deserunt.

Special Consideration

Bacon ipsum, dolor sit amet, ut et dui, meatball commodo ham salami, labore bacon, officia id excepteur, Velit doner meatball, deserunt.
<table>
<thead>
<tr>
<th>Section</th>
<th>Topic</th>
<th>Finding Name</th>
<th>Details</th>
<th>Past Findings</th>
<th>Type</th>
<th>Severity</th>
<th>Attachments</th>
<th>Required Actions</th>
<th>Finding Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>LHR-1</td>
<td>Anti-discrimination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Equal Opportunity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>Pregnancy Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>Medical Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LHR-2</td>
<td>Fair Treatment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Harassment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LHR-3</td>
<td>Prevention of Involuntary Labor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Forced Labor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2</td>
<td>Free to Leave</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3</td>
<td>Identification Surrender</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.4</td>
<td>Third Party Recruitment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5</td>
<td>Contracts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.6</td>
<td>Employment Fees</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LHR-4</td>
<td>Prevention of Underage Labor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>Underage Labor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Measuring Value of GRC - Reduced Risk

• Better risk mitigation
  – Speed of Decision Making
  – Reaction time to loss events reduced
    • Example: credit card data security breach – PCI non-compliance
  – Ability to understand co-relations of risks

• Assured compliance
  – Effective tracking and reporting
  – Detection and closure of gaps and deficiencies
  – Example: Penalty for noncompliance with laws

• Effective risk detection and assessment
  – Know where to focus, right prioritization
  – Translate assessment into actionable recommendations
  – Example: Positional intellectual property liability
Measuring Value of GRC - Lower Ongoing Costs

- **Reduction on**
  - Eliminate redundant and irrelevant activities
    - Harmonization of controls (for example Cobit, ISO 27002, PCI, SOX)
    - 20-40% reduction

- **Rationalizing Resources**
  - Consolidation and better resource utilization – lesser manual work
  - Improved assurance with current staff

- **Reduction in external costs of assurance**
  - Less use, more effective use with easy access to information
  - Estimated 25% savings in External Costs of Assurance

- **Lower IT costs**
  - Common infrastructure across various assurance groups
  - Faster compliance by system consolidation, information visibility
Measuring Value of GRC - Better Business Decisions

- **Reputation Management**
  - Preserving brand and shareholder value
    - Unmanaged incident, compliance issue - millions in reputation damage

- **Revenue Management**
  - Ensuring you don’t lose your customers
    - Customer loss - millions in revenue loss

- **Visibility**
  - Faster decision making
    - Pre-empted controls can result in hundreds of thousands in savings

- **Transparency**
  - Risk intelligence to board and investors

- **Strategic Value**
  - Align IT to business
  - Business performance gains through process standardization
Succeeding at Integrated GRC: Role of Platform

- **Configurability**
  - Modify data model, workflows, reporting for specific business needs

- **Extensibility**
  - Start in one area, extend seamlessly into others

- **Enterprise readiness**
  - Reliability, Availability, Scalability, Cloud and On-Premise Support

- **Multi-level security & access controls**
  - Multiple layers of hierarchy, business units spanning geographies

- **Integration mechanisms**
  - Big Data, Web Services, file upload, database, message bus, etc.
Summarizing: Next Steps in GRC

- Common information model
  - Multiple sites, regulations, functions, countries

- Collaboration driven
  - Standardized data collection to eliminate errors and inconsistencies
  - Manage compliance, risk and audits as a central function

- Integrated and real-time information flow
  - Leveraging internal and external sources

- Decision making and performance management
  - Easy access to analytics - with minimal manual work

- Tied to a closed-loop remediation, corrective actions processes
  - Seamless integration between compliance, risk and audit process
Thank you