MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

KPMG

cutting through complexity

WELCOME →

MetricStream GRC Summit 2013: Case Study

ENGAGE | INSPIRE | TRANSFORM

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

KPMG
cutting through complexity

Cutting through Complexity During Your GRC Journey

Angela Hoon

Principal | KPMG LLP

Lisa Rawls

Director | KPMG LLP

Supradeep Appikonda

Director | *MetricStream*

ENGAGE | INSPIRE | TRANSFORM

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

Agenda

- Introductions
- Teaming for a Successful GRC Journey
- Key Business Considerations
- Spotlight 1 – GRC Strategy & Governance
- Spotlight 2 – Convergence & Foundational Elements
- Spotlight 3 – Business Process Design
- Key Learnings and Best Practices
- Audience Questions and Discussion

ENGAGE | INSPIRE | TRANSFORM

KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

Introductions

MetricStream

Supradeep Appikonda

KPMG

Angela Hoon, Principal

Lisa Rawls, Director

ENGAGE | INSPIRE | TRANSFORM

KPMG MetricStream

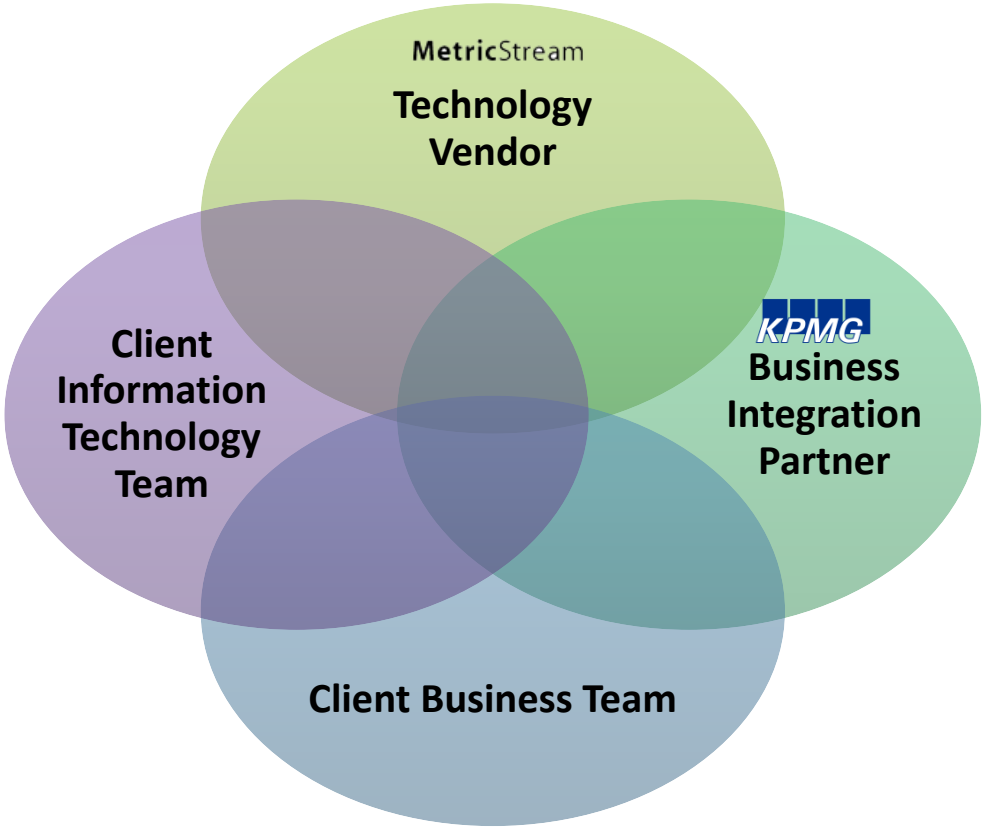
MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

Teaming for a Successful GRC Journey

KPMG and MetricStream work hand-in-hand to provide both technology and business support throughout the GRC Implementation process.



ENGAGE | INSPIRE | TRANSFORM

KPMG MetricStream

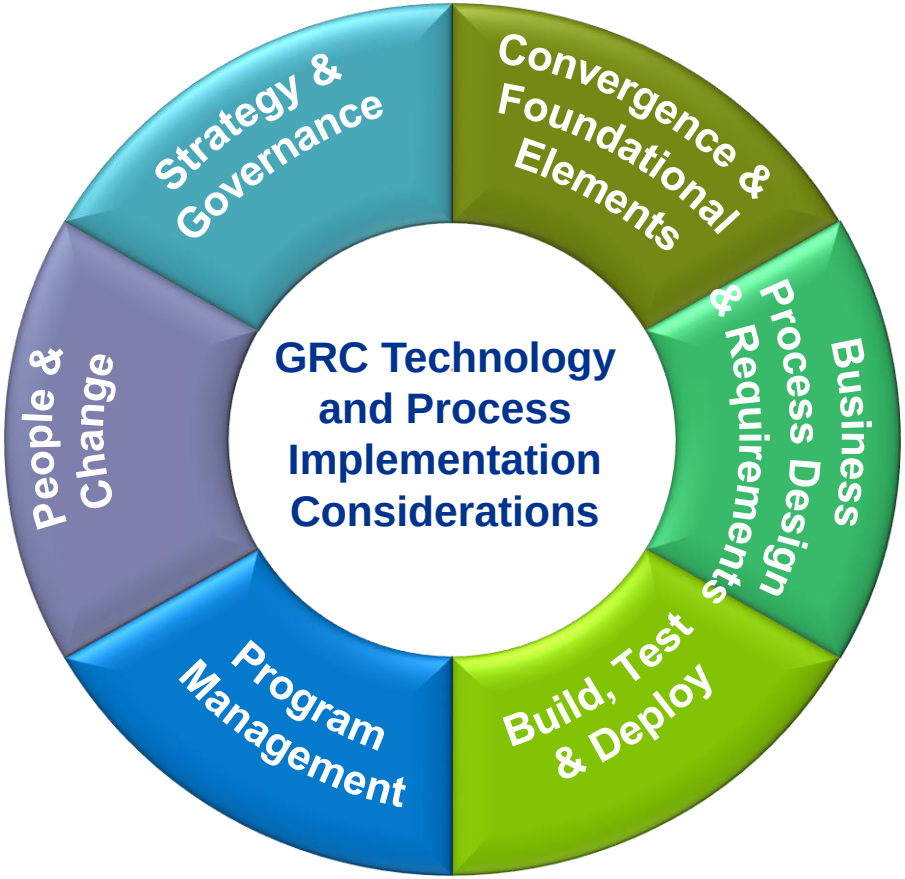
MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

GRC Technology and Process Implementation Considerations

A comprehensive view of GRC is needed to understand the implications of GRC on an organization.



ENGAGE | INSPIRE | TRANSFORM

KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

Key Business Considerations

A comprehensive view of GRC is needed to understand the implications of GRC Technology Implementation on an organization.

ENGAGE | INSPIRE | TRANSFORM

KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

Targeted Spotlights

Spotlight #1
GRC Strategy & Governance

Spotlight #2
Foundational Elements

Spotlight #3
Business Process Design

ENGAGE | INSPIRE | TRANSFORM

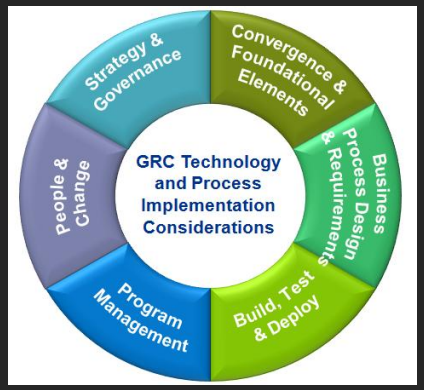
KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

GRC Strategy & Governance



ENGAGE | INSPIRE | TRANSFORM

Spotlight 1 – GRC Strategy & Governance

Client Challenge

- Lack of an overarching governance structure to support the implementation of an enterprise GRC solution at a company with recent acquisition
- Historic process to fund technology, make changes to technology no longer relevant at new company as additional parties now involved
- Lacked tactical process to aide in decision making of when and how new users groups will join technology user base
- Owner of the GRC initiative and technology not specified

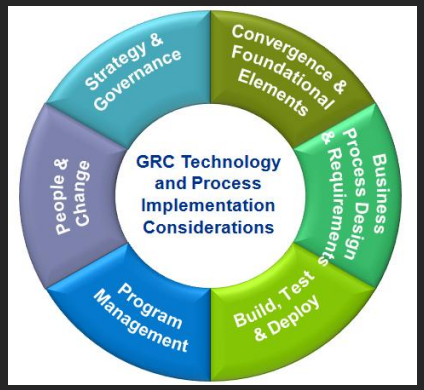
KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

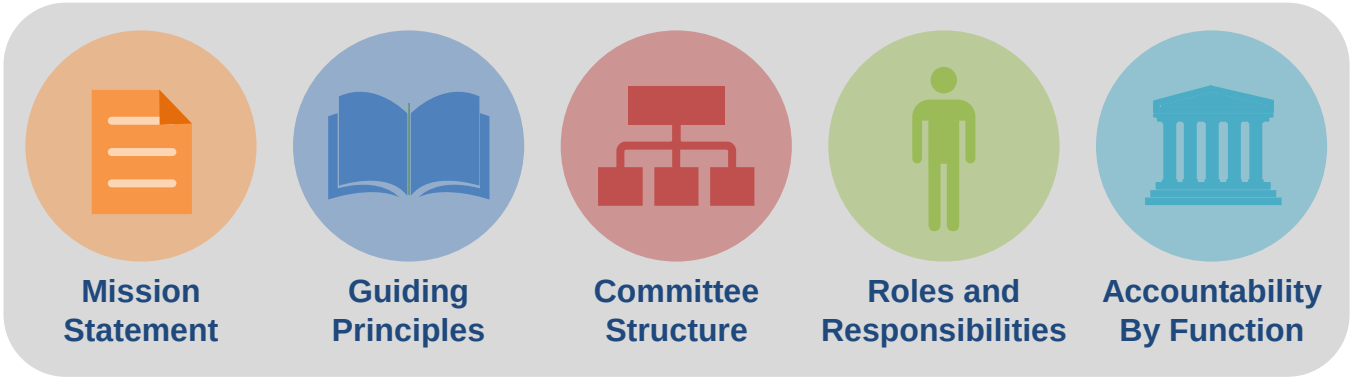
GRC Strategy & Governance



ENGAGE | INSPIRE | TRANSFORM

Spotlight 1 – GRC Strategy & Governance

KPMG assisted with the creation of a GRC Governance Plan to align assurance functions and support their GRC program and MetricStream technology.



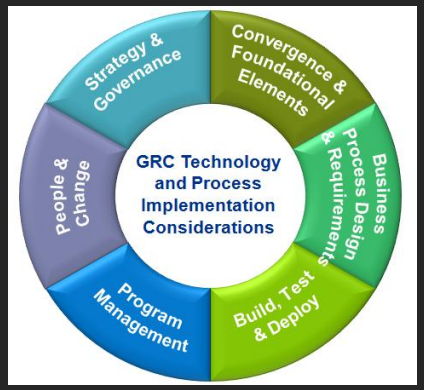
KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

GRC Strategy & Governance



ENGAGE | INSPIRE | TRANSFORM

Spotlight 1 – GRC Strategy & Governance

Solution:

- Gained buy in form executive leadership through tactical GRC support team
- Created a Governance structure to support the GRC program and the MetricStream technology

Benefits:

- Roles and responsibilities now formalized and communicated throughout user group
- Process enabling all to have a voice at the table formalized
- Support structure in place to allow for future roll-out of the GRC technology to additional user groups
- Group now formalized to govern future changes to technology and establish the common terminology
- Ultimately, assisted with breaking down silos

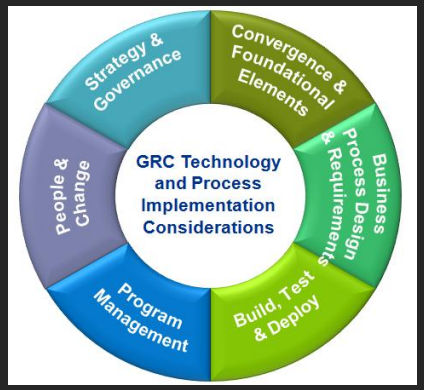
KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

Convergence & Foundational Elements

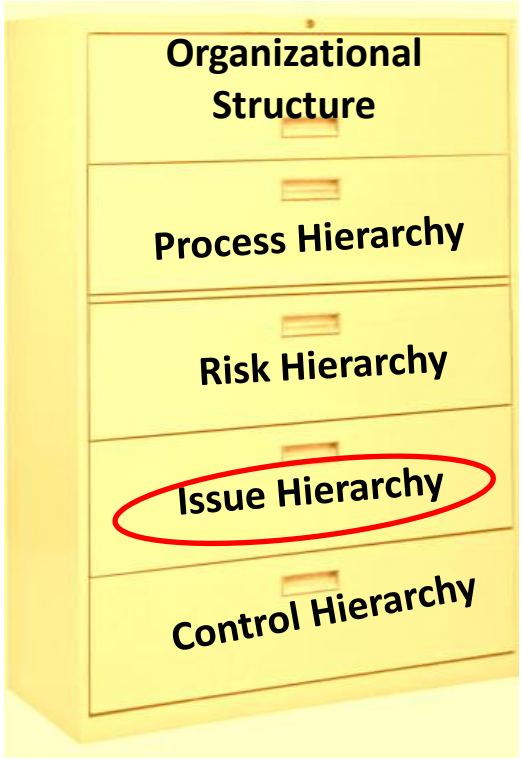


ENGAGE | INSPIRE | TRANSFORM

Spotlight 2 – Convergence & Foundational Elements

Client Challenge:

- Multiple groups including, migrating to shared MetricStream platform in one to three years.
- No common taxonomies or language – ratings currently defined and used across user groups



User Group Issue Terminology

Compliance
- Reportable
- Non-Reportable
- Process Improvement

Internal Audit
- High
- Medium
- Low

Information Security
- Critical
- High
- Medium
- Low

SOX
- Material Weakness
- Significant Deficiency
- Deficiency

ERM
- Critical
- Major
- Moderate
- Minor
- Insignificant

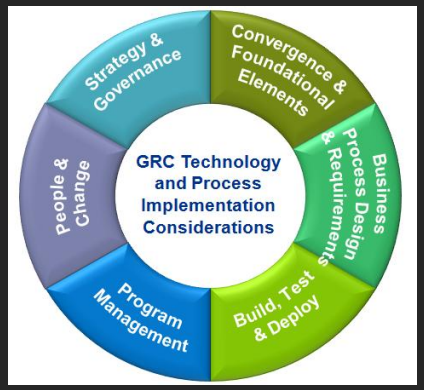
KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

Convergence & Foundational Elements



ENGAGE | INSPIRE | TRANSFORM

Spotlight 2 – Convergence & Foundational Elements

KPMG helped align issue priorities and ratings across the key functions.

	ERM	Audit	Compliance	SOX	Info Sec
BLUE - 1	Insignificant				
GREEN - 2	Minor	Low	Low		Low
YELLOW - 3	Moderate	Medium	Medium	Control Deficiency	Medium
ORANGE - 4	Major	High	High	Significant Deficiency	High
RED - 5	Critical		Critical	Material Weakness	Critical

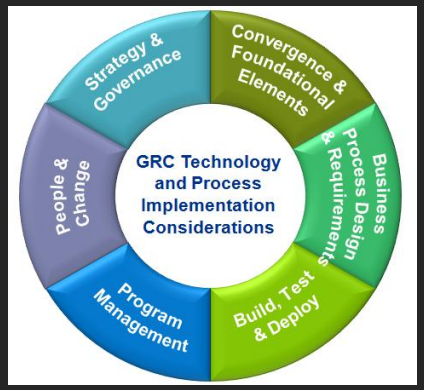
KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

Convergence & Foundational Elements



ENGAGE | INSPIRE | TRANSFORM

Spotlight 2 – Convergence & Foundational Elements

KPMG helped build the agreed upon foundational elements, including establishing a common language for issue priority.

BLUE - 1	• An issue that has little or no impact on the current environment but requires tracking
GREEN - 2	• An issue that represents a minor control weakness or process improvement opportunity that requires communication at the **area or process level**
YELLOW - 3	• An issue, or combination of issues, that may result in obstacles to compliance with required regulation; loss of sensitive information, significant financial impact; which requires notification at the **divisional level**
ORANGE - 4	• An issue, or combination of issues, that may result in obstacles to compliance with required regulation; loss of sensitive information, significant financial impact; which requires notification at the **executive level**
RED - 5	• An issue, or combination of issues, that may result in obstacles to compliance with required regulation; loss of sensitive information, significant financial impact; which requires notification at the **senior executive/board level**

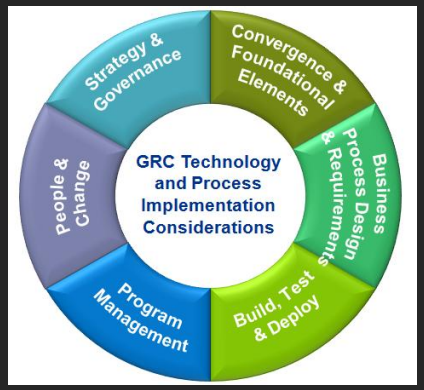
KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

Convergence & Foundational Elements



ENGAGE | INSPIRE | TRANSFORM

Spotlight 2 – Convergence & Foundational Elements

Solution:

- Defined common language and the foundational elements
- Obtained input and agreed from all groups using the MetricStream system in the future

Benefits:

- Promoted common language in the culture, used daily across organization, even prior to technology go-live
- Increased efficiencies for aggregation of reporting across multiple groups
- Streamline the process of business requirements, specifically over issue management

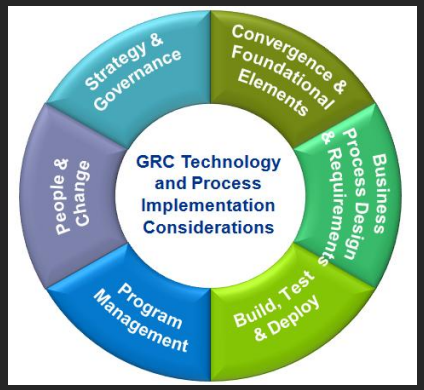
KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

Business Process Design & Requirements



ENGAGE | INSPIRE | TRANSFORM

Spotlight 3 – Business Process Design

Client Challenge:

- Initiative underway to develop a new ethics and compliance risk assessment process including :
  - Risks
  - Compliance Controls
  - Compliance Gaps/Issues
  - Remediation Activities
  - Control Test

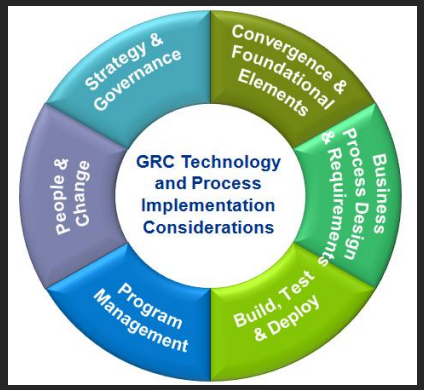
KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

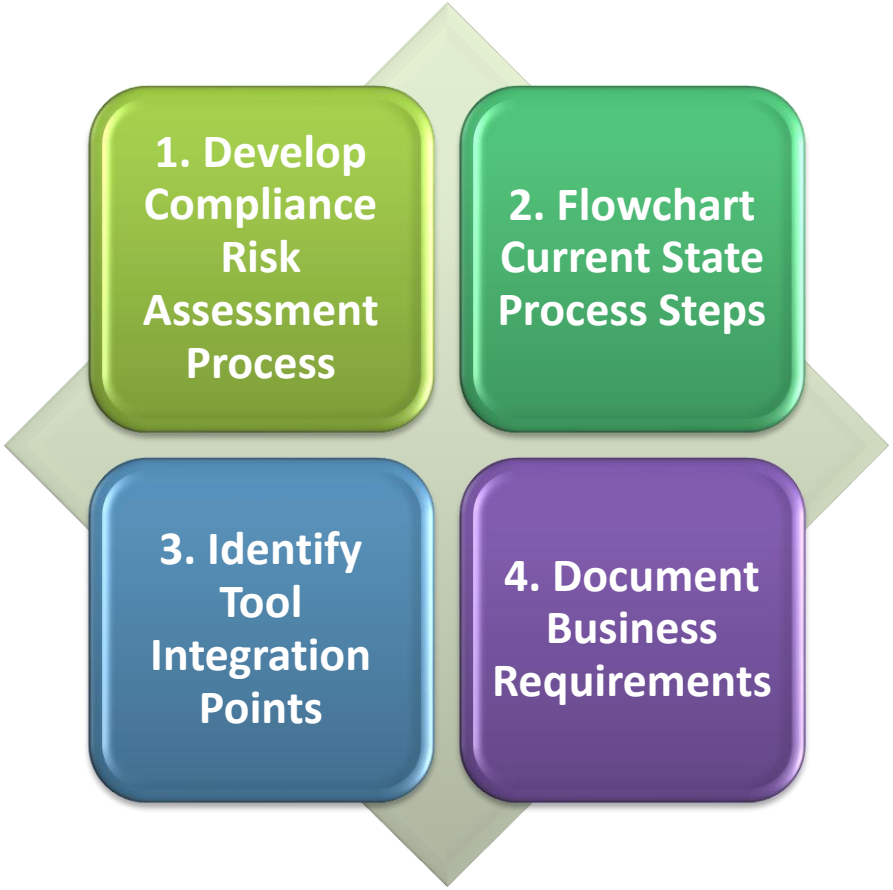
Business Process Design & Requirements



ENGAGE | INSPIRE | TRANSFORM

Spotlight 3 – Business Process Design

KPMG supported the identification of the high-level steps required to build the Compliance Risk Assessment process.



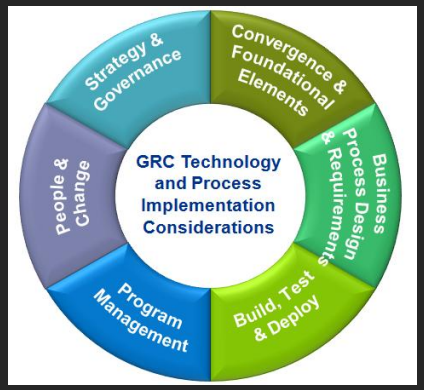
KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

Business Process Design & Requirements



ENGAGE | INSPIRE | TRANSFORM

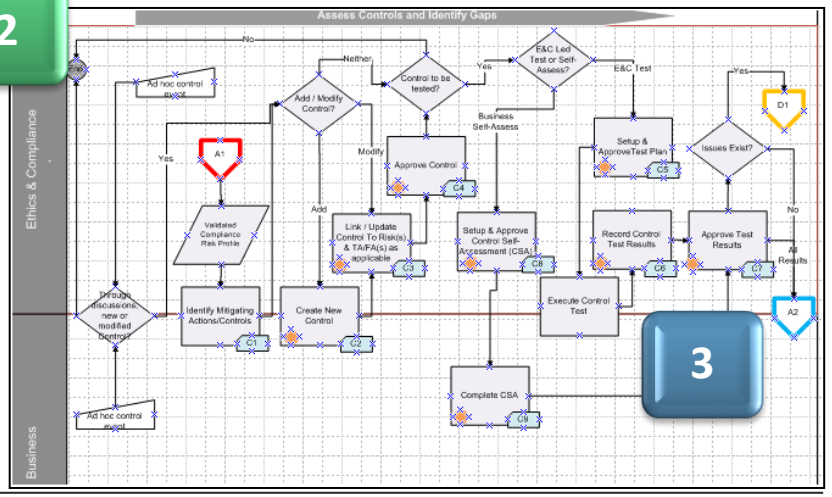
Spotlight 3 – Business Process Design

KPMG created the detailed process flow, highlighting the specific steps in the process, who would perform them, and those which can be enabled via the MetricStream technology.

1

1. Business Area Led Data Gathering
2. Ethics and Compliance Risk Aggregation
3. Business Area Leadership Validation
4. Identification and Assessment of Controls/ Risk Management Actions
5. Reporting

2



3

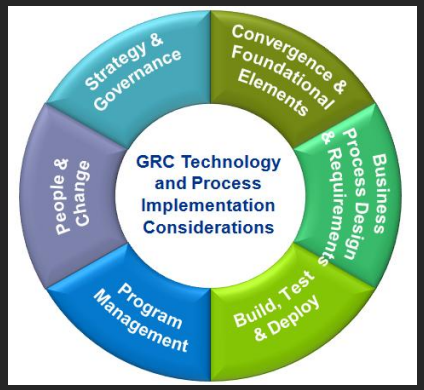
KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

Business Process Design & Requirements



ENGAGE | INSPIRE | TRANSFORM

Spotlight 3 – Business Process Design

Solution:

- Assisted with building the high-level steps in the process
- Developed the detailed process flow diagrams that highlighted which steps could be enabled via technology

Benefits:

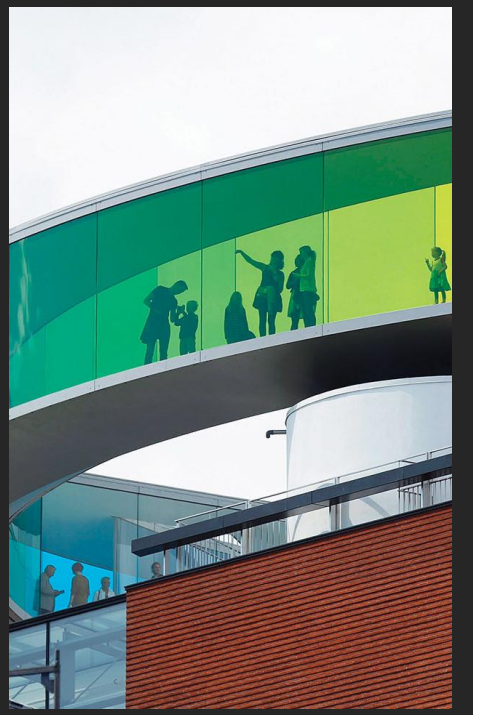
- Ability to more readily define business requirements, focusing on those that were to be enabled via technology
- Supplied detailed requirements and process flows to MetricStream in a language that is understandable by both the business and MetricStream
- Process for executing risk assessment and compliance management activities will be enabled via MetricStream technology in the future
- Risk and compliance information will be stored centrally, increasing reporting efficiencies

KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV



ENGAGE | INSPIRE | TRANSFORM

Key Learnings and Best Practices

- **Include all relevant stakeholders at the start of the project**
- **Develop a formalized GRC Governance structure**
- **Gain agreement from all stakeholders on 'Foundational Elements' prior to business requirements**
- **Define and agree upon future state process prior to defining business requirements**
- **Establish a clear project plan inclusive of change and risk management**
- **Establish a cohesive change management and communications plan**
- **Do not let a tool drive the process!**

KPMG MetricStream

MetricStream

GRC SUMMIT 2013

Apr 30 - May 1, 2013 | Mandarin Oriental, Las Vegas, NV

KPMG
cutting through complexity

Questions and Discussion

ENGAGE | INSPIRE | TRANSFORM

Angela Hoon

ahoon@kpmg.com

Lisa Rawls

lisarawls@kpmg.com

Supradeep Appikonda

Supradeep@MetricStream.com