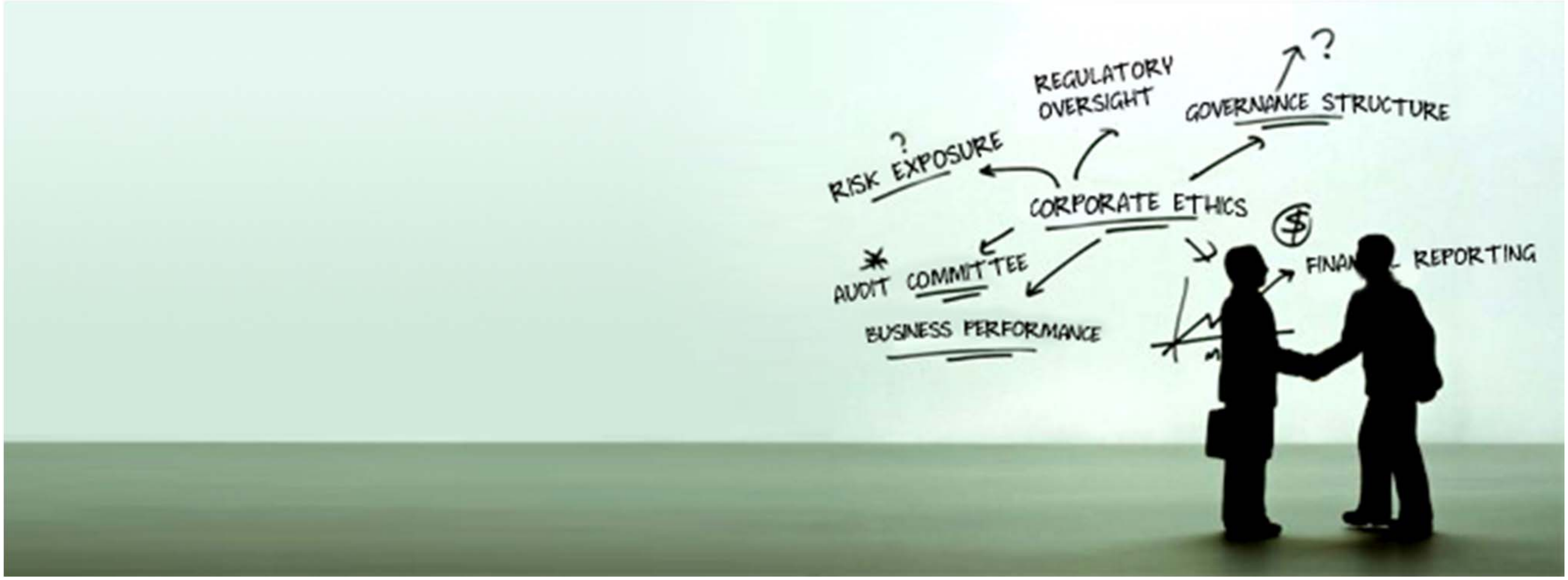


DUBAL’s ISO 31000-based ERM Program

Building a Harmonized, Proactive and Sustainable Approach to Risk Management

October, 2013

Toby Shore
Corporate Treasurer &
Chief Risk Officer
DUBAL

MetricStream

Key Things To Discuss Today…

- Enterprise Risk Management – An industry perspective
- Establishing the Risk Management process
- Four technology solution evaluation criteria
- Features of a mature Risk Management Solution
- Best practice from implementing an ERM Solution

ENTERPRISE RISK MANAGEMENT AT DUBAL

Toby Shore
Corporate Treasurer and Chief Risk Officer

Together we shine
www.dubal.ae

dubal
Dubai Aluminium

Enterprise Risk Management – 10 Common Misconceptions

- Inherent risk is a workable basis for ERM;
- Risk management is an end unto itself, independent of business objectives;
- Risk tolerance is the same as risk appetite;
- Risk management can be decentralised and done piecemeal;
- One skill set is enough;
- ERM is a low-level treasury or finance project;
- All risks are equally important;
- Managing upside risk is a routine focus of ERM;
- ERM has no discernable effect on financial markets or firm value;
- ERM is primarily a response to Sarbanes Oxley

…most of these errors of thinking or execution stem from a common source: the failure to recognise that ERM is in fact an easier, simpler and more logical undertaking than most people realise.

Source: John Fraser & Betty Simkins; Journal of Applied Corporate Finance [2007]

Enterprise Risk Management – Establishing The Context

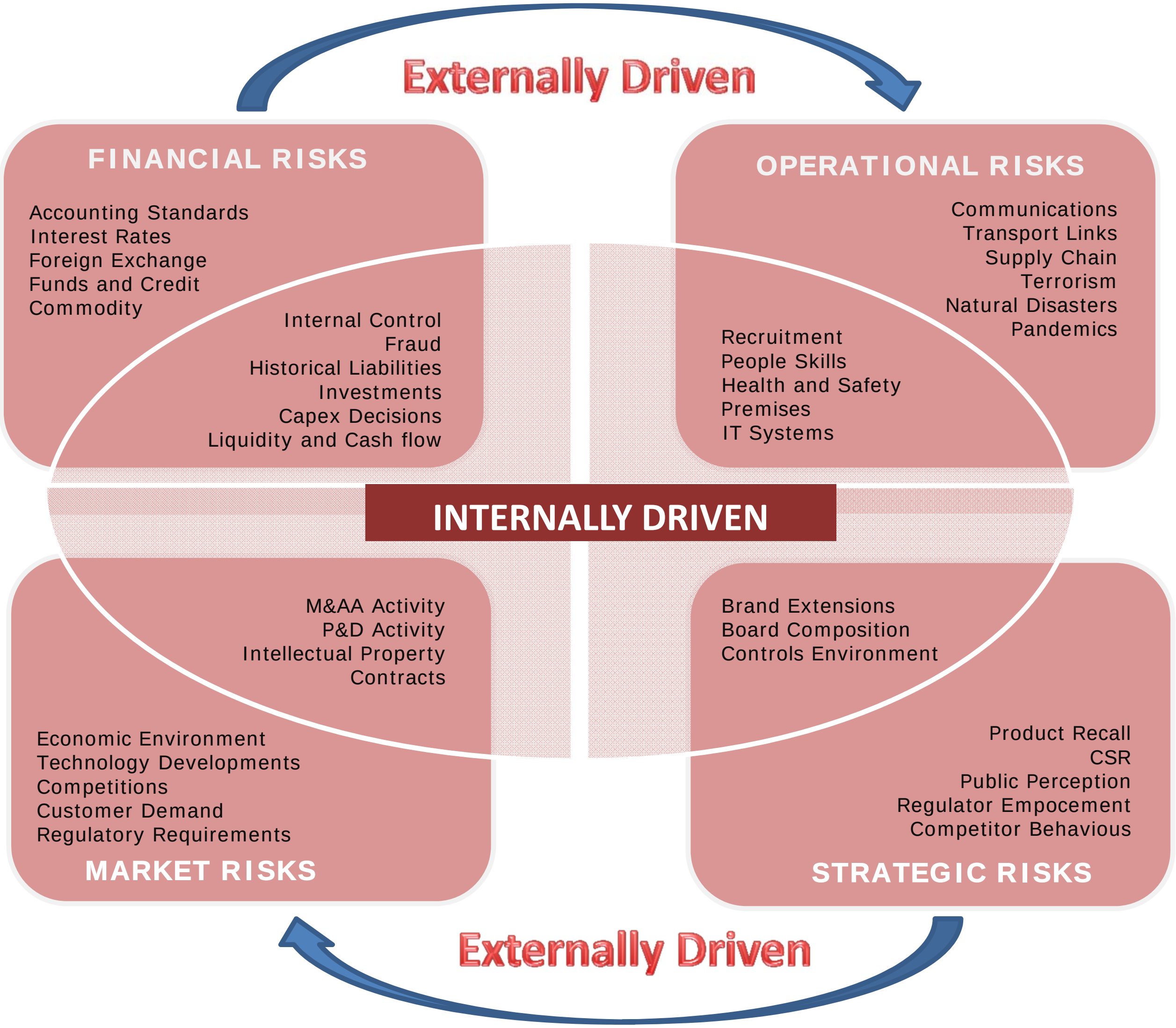
- Risk, under ISO 31000, is defined as ***the effect of uncertainty on objectives*** - it may be positive, negative or simply a deviation from the expected.

- The key objective of DUBAL's enterprise wide risk management framework is to ensure that effective risk management policies, strategies and processes are in place and its primary purpose is to protect and enhance shareholder value.

- Within DUBAL there are many inherent risks:
  - some which we mitigate and control,
  - some which we share with 3rd parties,
  - some which we manage *and*
  - some which we simply accept.

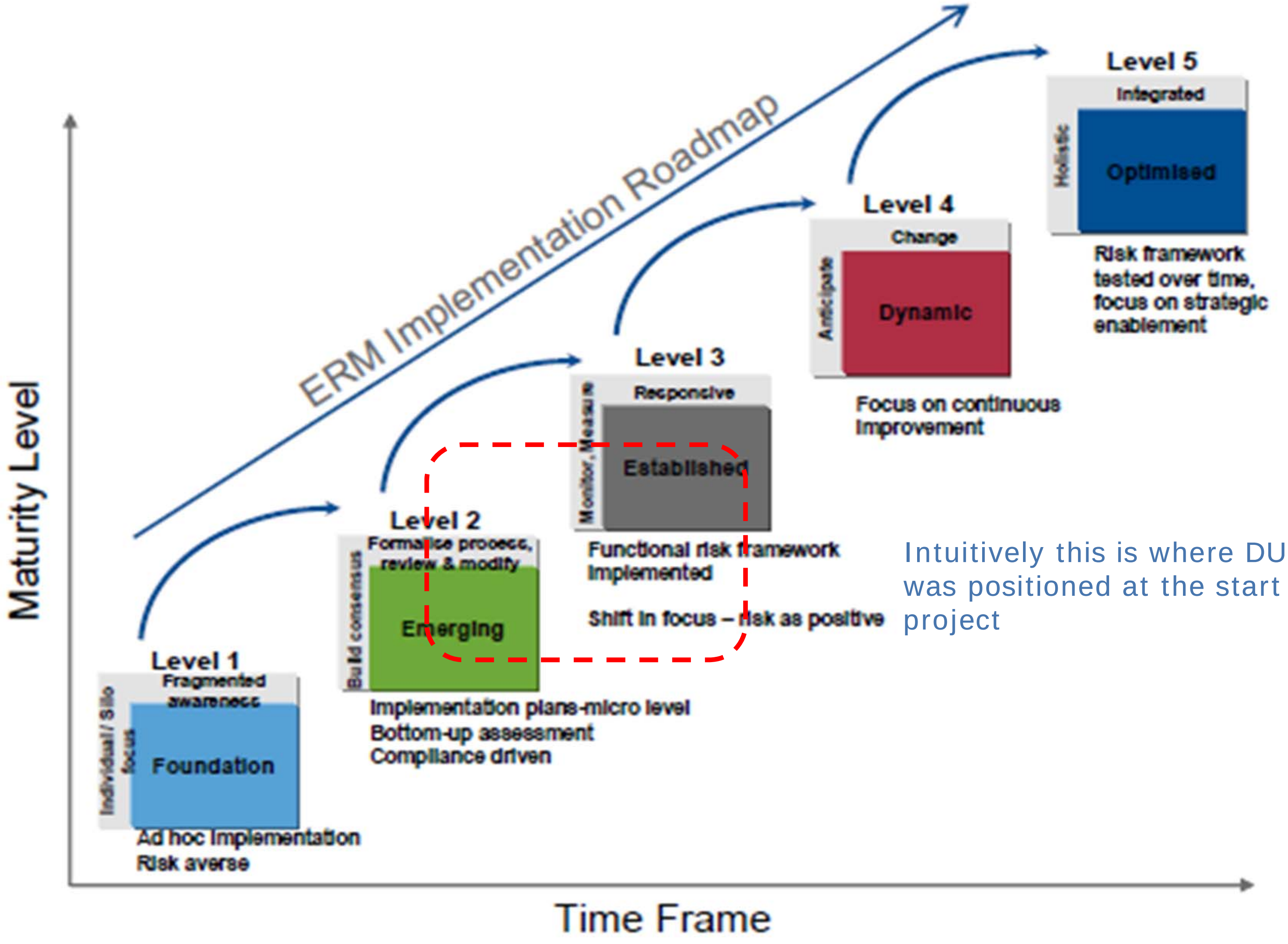
- DUBAL categories its risks as follows:
  - Financial
  - Operational
  - Market
  - Strategic / Reputational

Enterprise Risk Management – Establishing The Context



Adopted from: AIRMIC & IRM, 2010

Enterprise Risk Management – Maturity Assessment



Intuitively this is where DUBAL was positioned at the start of the project

ERM Maturity Assessment Framework

Source: The Willis Group

Enterprise Risk Management - Process

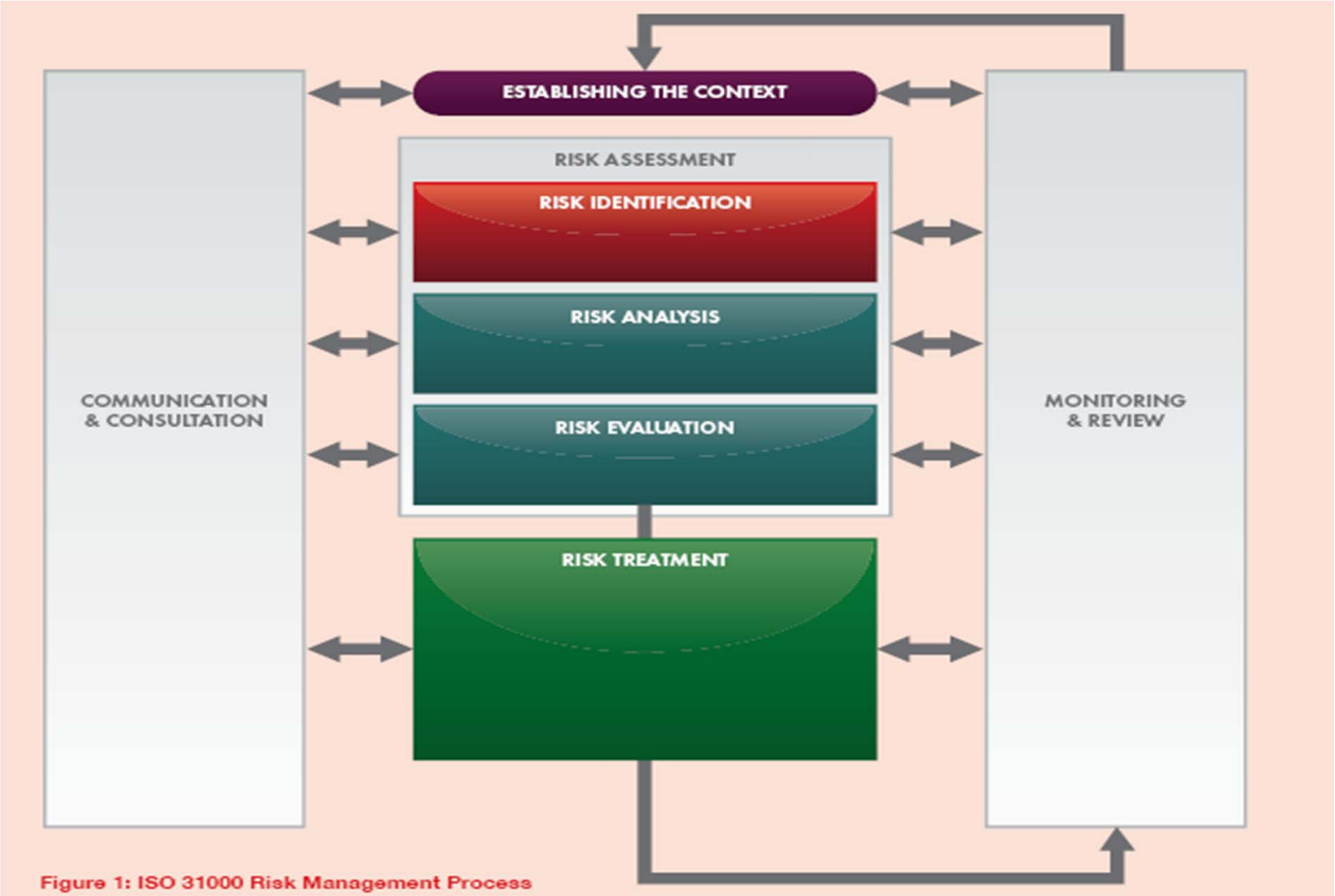


Figure 1: ISO 31000 Risk Management Process

Enterprise Risk Management – Process

Step 1:

Top 50 – 60 Business Unit Risks identified, collated and evaluated:

- Very High
- High
- Medium
- Low
- Very Low

Step 2:

Transition to quantitative assessment of Top 50 – 60 Business Unit Risks using 3 point estimate:

- **Minimum** Anticipated Financial Impact
- **Anticipated** Financial Impact
- **Maximum** Anticipated Financial Impact

Step 3:

Monte Carlo Simulation exercise on Top 50 – 60 Business Unit Risks

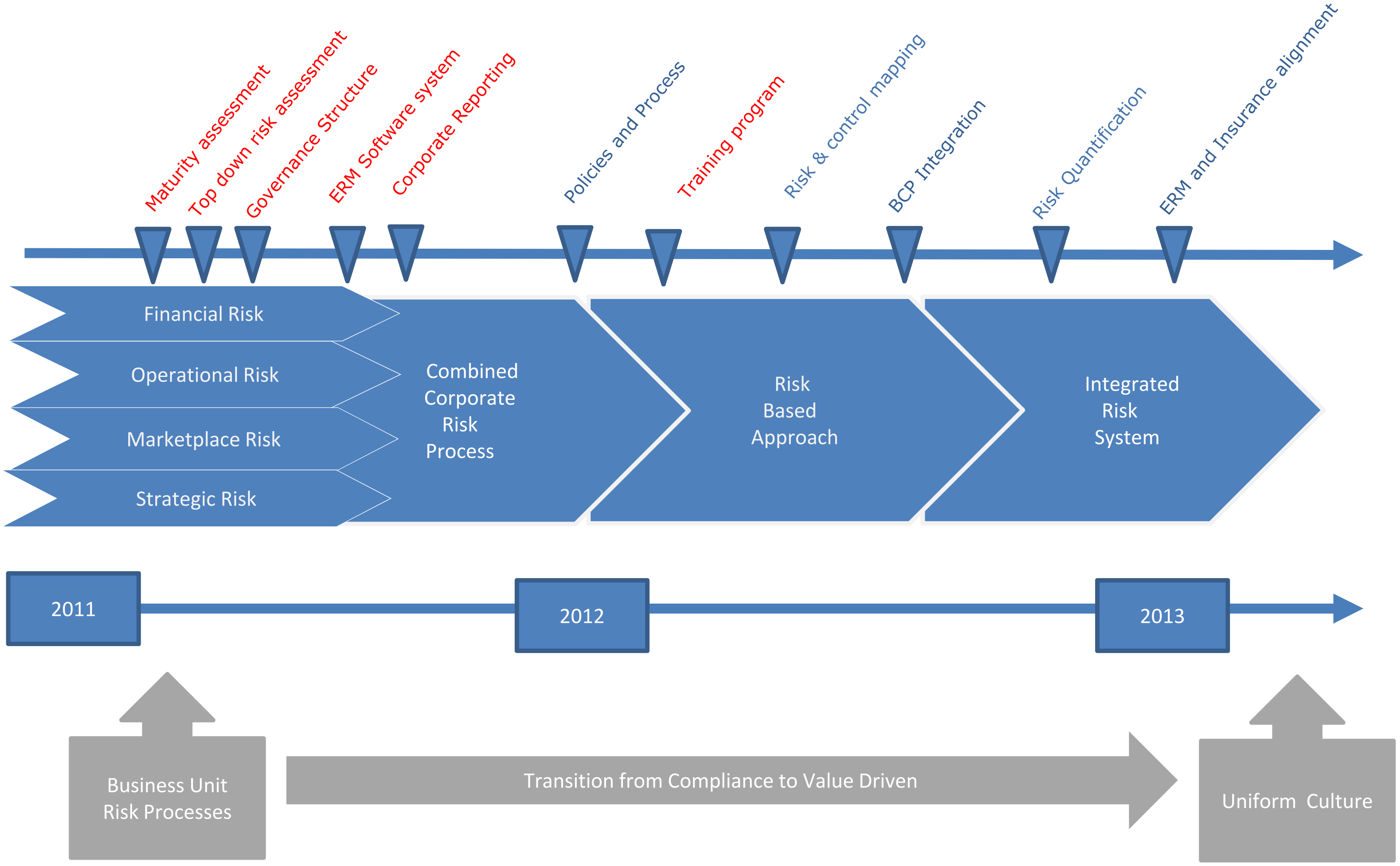
Step 4:

All Business Unit risks identified, collated and evaluated using a mix of both qualitative and quantitative assessments.

Step 5:

Monte Carlo Simulation on all identified risks

Enterprise Risk Management – A Structured Roll-out



Enterprise Risk Management – System Selection

- In Q4 2011, DUBAL undertook an extensive tendering process involving six (6) vendors;

- Following evaluation of initial proposals, a short-list of three (3) vendors were invited for product presentations and demonstrations of solution delivery;

- MetricStream were the successful vendors and a scoping and blueprinting exercise was held in January 2012;

- Due to the requirement from the DUBAL Board for a Enterprise Wide Risk Report to be presented in April, the go-live date was scheduled for 31 March 2012 and this was met on time;

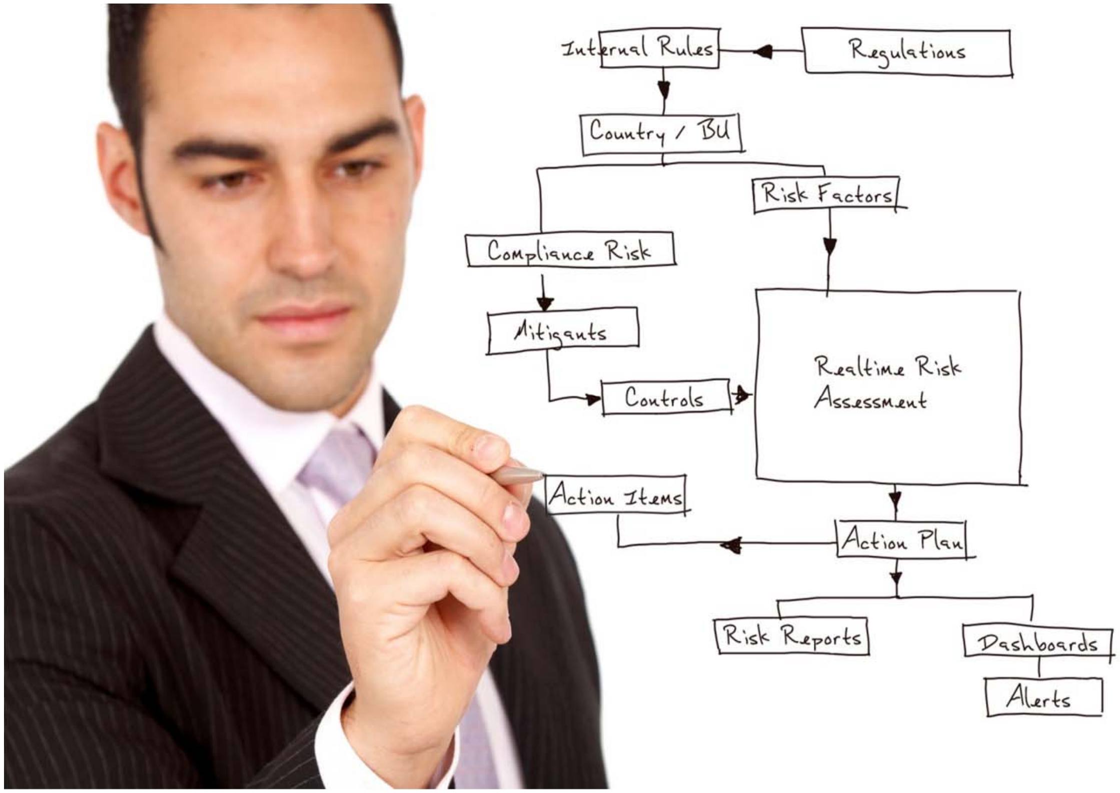
Enterprise Risk Management – Why MetricStream ?

DUBAL’s evaluation method centered around four key criteria:

- **Flexibility of product customization**: Each ERM implementation is unique and depends on philosophy, framework and risk appetite. MetricStream consistently demonstrated a flexible approach towards product customization to match DUBAL’s requirements;
- **Highly Integrated GRC Platform**: MetricStream is tightly integrated between Risk, Internal Control and Internal Audit allowing DUBAL to leverage synergies whilst ensuring operational independence;
- **Rich functionality**: MetricStream demonstrated an ability to meet all of DUBAL’s key requirements including data driven Key Risk Indicators [KRI’s] and quantitative risk analytics; *and*
- MetricStream is well positioned in the **Leaders Quadrant in Gartner’s Magic Quadrant** for Enterprise Governance, Risk and Compliance platforms.

Together we shine

Professional Passionate Versatile Trustworthy Caring Innovative



Best Practices in Implementing Internal Control & Risk Management at DUBAL

Prashant Rao Murari
Head of Professional services - International Business
MetricStream

DUBAL’s Need for Internal Control & Risk Management

ERM Objectives

- To ensure that all the current and future material risk exposures of DUBAL are identified, assessed, quantified, mitigated and managed appropriately
- To ensure protection of shareholder value through establishment of an integrated framework for the company’s risk management process and to ensure companywide implementation
- To assure business growth with financial stability
- To provide clear and strong basis for informed decision making at all levels of the organization
- To continually strive towards strengthening the Risk Management System through continuous learning and improvement

Internal Control Objectives

- Assess the “design” and “effectiveness” of the company’s internal controls that relate to all systems and business processes that have an effect on achieving our business objectives and / or have an effect on significant balance sheet and P&L accounts
- Identify opportunities to streamline business processes, wherever feasible

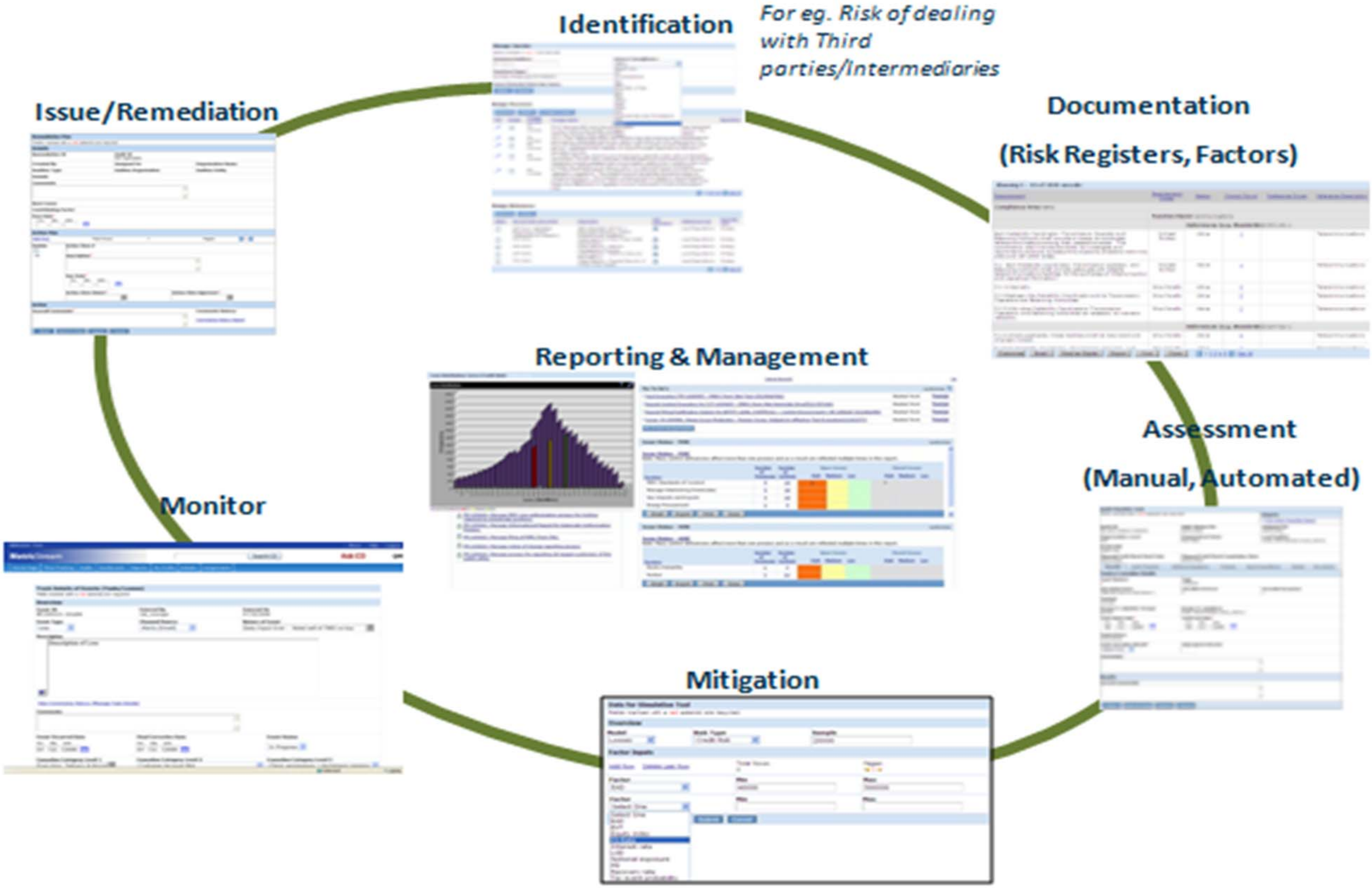
The Proposed Solution

MetricStream implemented an integrated ERM solution consisting of:

- Risk Assessment and Analysis
- Compliance Management and Control Assessments
- Scenario Modeling and Monte Carlo Simulation
- Risk-control Library
- Risk and Control Monitoring
- Loss Management
- Issue Management

Identify
Assess
Plan
Implement
Communicate

Risk Management Solution Overview



Identification

For eg. Risk of dealing with Third parties/Intermediaries

Documentation

(Risk Registers, Factors)

Assessment

(Manual, Automated)

Mitigation

Monitor

Issue/Remediation

Reporting & Management

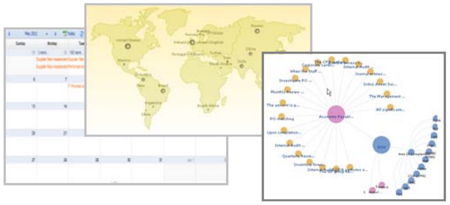
Risk Management: Key Strengths

- Flexible and adaptable Risk and Control framework
  - Based on industry standards such as ISO, COSO, COBIT Standards etc.
- Quantities and Qualitative Risk Assessments, Scenario modeling
- Advanced Risk Modeling capabilities
  - Visualization, mitigation strategies, risk relationships & scoring
- Internal and external Loss event management
  - Event recognition, investigations, remediation, loss data analysis
- Key Risk Indicators (KRIs) for tracking risk metrics and thresholds
  - Automated notification when thresholds are breached

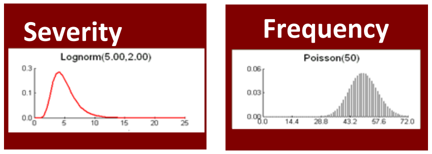
Risk Intelligence for Business Performance

Reporting & Analytics

Report & Dashboarding



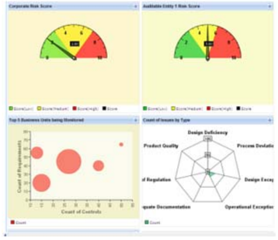
Advanced Data Visualizations



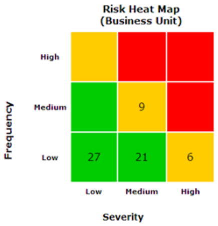
Plug ‘n Play Analytics

Risk Metrics, KRIs / KPIs & Business Objectives

KRIs, KPIs



Business Objectives



Heat Maps

GRC Processes

- Risk Assessments
- Control Tests
- Self Assessments
- Audits
- Policy Management
- Surveys
- Monitoring
- Issue Management

Internal & External Data

Organizational Data

Loss Data

Threats & Vulnerabilities

(Servers/Computers/Mobile/Cloud Assets)

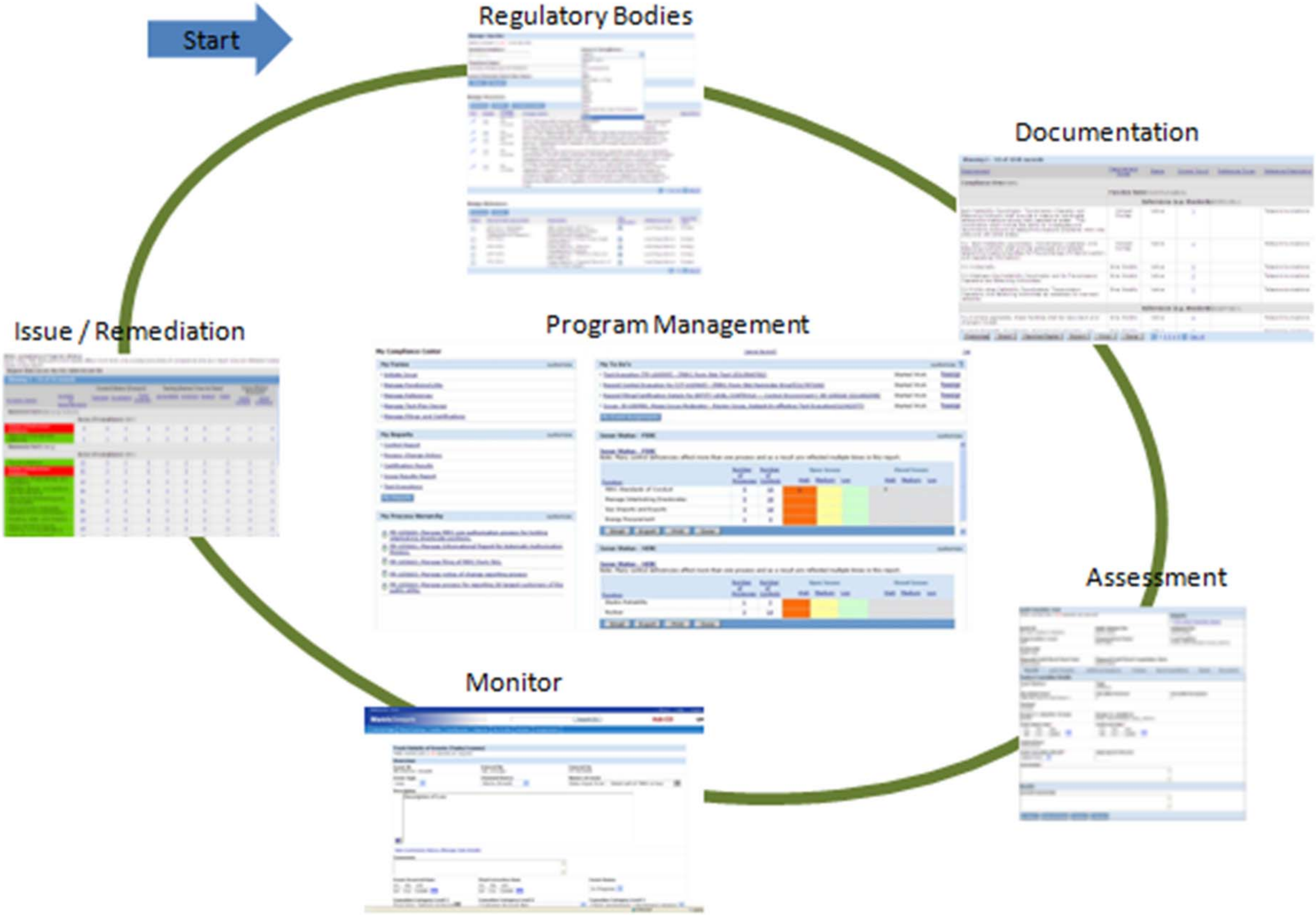
ComplianceOnline Content

External Feeds

(Regulatory Updates, Social Monitoring, etc.)

MetricStream

Internal Control Management Solution Overview



Start

Regulatory Bodies

Documentation

Assessment

Monitor

Issue / Remediation

Program Management

Internal Control Management Solution – Key Strengths

- Common framework for multiple compliance requirements
  - Cross-industry mandates and regulations: SOX, OSHA, EH&S, FCPA, IT, ISO, NIST, COSO, COBIT…
  - Industry focused regulatory guidelines: FDA, FERC, FAA, HACCP, AML, Basel II, CIA, Medicare, RAC, Solvency II
- Control monitoring and enforcement
  - Assessments, tests, audits, surveys
- Powerful compliance monitoring and reporting
  - Including regulatory submissions
- Integrated regulatory intelligence
  - Compliance alerts triggered workflows

Key Benefits

DUBAL's ERM program, supported by the MetricStream GRC solutions, has:

- **Improved standardization:** With streamlined and harmonized multiple risk management processes across the enterprise
- **Increased collaboration and accountability:** Breaking down organizational silos & improving the efficacy of decision-making
- **Increased risk protection:** Enabling decision makers to quickly determine the potential impact of risk and develop action plan
- **Integrated, Real-time View of Risks:** Advanced risk heat maps, charts, dashboards, and trending analyses that strengthen transparency into risk and control management
- **Improved risk management Maturity for Compliance with ISO 31000 Standards:** Through a structured and systematic approach to risk management
- **Delivered greater efficiency and reduced costs:** Automating multiple manual processes such as risk-control assessment, reporting, remediation, and audit trails

Thank You

Contact:
Email: info@metricstream.com
Phone: Switzerland – +41-615-880-111 |Australia – +61-870-708-014
United Arab Emirates - +971-2-4040700 | United States – 1 650.620.2955

MetricStream