24th XBRL International Conference

“Transparency: with Available, Reliable, Comparable and Re-usable Data”

March 20-22, 2012
Abu Dhabi, UAE

ORSA Track
Enabling Governance, Risk and Compliance Information Sharing with XBRL Technology
Said Tabet and John Dill
Thursday, 22 March 2012
AGENDA

- Brief Overview
- What is GRC?
- Business Case
- GRC–XML Working Group
- GRC and XBRL
- GRC–XML Taxonomy and Information Model
A Transformational Opportunity For All Stakeholders

**Current State**
- Fragmented silos
- Mostly reactionary
- Individual projects
- Separate from mainstream processes and decision-making
- Spreadsheets, spreadsheets, spreadsheets
- Limited and fragmented use of technology

**Future State**
- Integrated management & performance
- Proactive planning & execution
- Integrated capability
- Embedded within mainstream processes and decision-making
- Coordinated transactions & shared data
- Architected solutions
GRC Program Oversight

- Requirements are not new, but have expanded
- Automation and standardization is a trend and opportunity
- Historically required of Managed Service Providers (MSP):
  - IT Service Level Agreements with metrics
  - IT Service Management
  - Business Continuity
  - Compliance certification against a framework such as ISO27001/2
A common language of risk and control is a prerequisite for effective management of audit, risk, and compliance processes.

Most organizations currently struggle with a common language of risk and control between their internal GRC silos.

There is no standard risk and control language for multiple information systems to communicate or pass information.
Overview (Cont’d)

- Standard risk and control models exist and are utilized by many organizations (COSO, COBIT, ITIL, ...), yet there is no common language for systems to communicate on these taxonomies.

- XBRL is a functional technology for enabling systems to communicate business and financial reporting information.

- XBRL can be effectively leveraged to enable information systems to communicate Risk, Control and Test of Control information.

**GRC-XML is a framework for the exchange and sharing of Governance, Risk, and Compliance Information**
GRC–XML Mission

As a working group, we focus on

- Creating the next version of the GRC–XML Taxonomy Framework
- Providing guidance and support to enable tooling and prototyping in order to demonstrate how standard libraries can be integrated and translated to GRC–XML, where possible.

We expect vendors and other organizations to create their own mappings between GRC–XML and their proprietary formats.
Scope and Taxonomy Requirements

- Enhance the current version of GRC-XML
- Define the GRC-XML requirement for Cloud environments (Security needs, Service level agreements, data governance, etc.)
- Refine and formalize vocabulary and update it as needed
- Ability to support conversion and versioning between the many standards and libraries that are available (ITIL, COSO, COBIT, NIST, UCF, Basel2/3, and proprietary libraries)
- Support the tagging and the traceability from the data layer all the way to the business level (goals, processes, objectives, policies, etc.)
- Use XBRL GL as the standard format for evidence and input, and XBRL FR for summarized reporting
Sample Deployment

Risk & Controls Repository
- Risk models
- Controls documentation
  - Organization / Process
  - Test Procedures
  - Test Results

Controls Testing & Monitoring
- Automated Control Tests
  - Transactions
  - Configurations
  - User access
- Manual Control Tests
  - Surveys
  - Sampling

GRC Applications & Systems
- Enterprise GRC,
  - Operational GRC,
  - IT GRC, etc.

GRC XML
- Flow between Risk & Controls Repository and Controls Testing & Monitoring
- Flow between Controls Testing & Monitoring and GRC Applications & Systems
Enabling transparency and traceability
Summary

- Integration of different areas: security risk, IT risk, financial risk, operational risk, and others – many areas, one language
- Visibility across silos
- Reduction of redundancies and duplications
- Standardization, simplification
- Reduced information friction to facilitate (more) continuous monitoring and audit of controls
- Consistency of Regulatory Supervision
- Facilitate Efficient Regulatory Oversight
To Get Involved

- Join our working group
- Collaborate with us:
  - Use Cases in your specific sector(s)
  - Reviews of published specification
  - Implement and support the standard

- Contact us:
  Said Tabet: stabet@oceg.org
  John Dill: jdill@bma.bm