Agenda

Overview
Governance Risk and Compliance
  Brief Introduction
Standards Initiatives
Business Standards, XBRL and GRC-XML
  XBRL and XBRL GL,
  eSupervision, ERM, Solvency II
  GRC-XML Taxonomy, Open Risk Universe
Summary
Overview

• Data is
  - Everywhere, structured, unstructured, complex,
  - In many forms and from multiple source

• Data Classification
  - Vocabularies, Taxonomies, Ontologies using open standards

• Data Processing, Automation
  - Search, Infer, Aggregate, Analyze, Manage
Overview (Cont’d)

• Cloud Computing
  - IT Evolution and 21st Century Enterprise Architecture?

• Big Data
  - The real challenges and the opportunity

• From Data to Knowledge
Enterprises today: The Problem
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
Why do we need Standards?

- Use of available technical expertise, enhanced trade
- Common metrics for service level expectations
- Essential to the cloud supply chain
- Open global markets
- Required by legal and accounting professions
- Increased automation
Foundations for Information and Knowledge Interchange
Foundations for Information Interchange

GRC-XML: What is it?

- Standard language for Risks and Controls definition/exchange
- One language for many areas:
  - Security risk
  - IT risk
  - Financial risk
  - Operational risk, etc.
- Visibility across silos
- Eliminate redundancy and duplication
- Facilitate effective continuous monitoring and audit of controls
- Extensible: Companies can add their own
  - Activities
  - Risks
  - Control Objectives
  - Control Activities, etc.
GRC-XML Information Model
Enterprise Risk management Process

Phase 0: Corporate Strategy
1. Risk Management Organization
2. Risk Management Charter

Phase 1: Risk Strategy
1. Risk Identification
2. Risk Tolerance (Risk Appetite) definition

Phase 2: Risk Assessment
1. Risk Evaluation
2. Risk Integration (Heat Mapping)

Phase 3: Risk Mitigation
1. Mitigation Planning
2. Mitigation Installation
## Enterprise Risk management Process using XBRL

<table>
<thead>
<tr>
<th>Phase</th>
<th>What you will do</th>
<th>XBRL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1 Risk Identification</td>
<td>Identify risks related to the organization, and select significant risks</td>
<td>Risk Universe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Extend to define significant risks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk Taxonomy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Risk Event</td>
</tr>
<tr>
<td>1-2 Risk Tolerance</td>
<td>Define risk level (impact/likelihood) and tolerance level to the significant risks</td>
<td>Risk Appetite</td>
</tr>
<tr>
<td>(Risk Appetite) definition</td>
<td></td>
<td>- Risk Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Risk Tolerance</td>
</tr>
<tr>
<td>2-1 Risk Evaluation</td>
<td>Evaluate the significant risks and identify existing controls</td>
<td>Risk Taxonomy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Risk Score</td>
</tr>
<tr>
<td>2-2 Risk Integration</td>
<td>Map the result of evaluation into Heat Map</td>
<td>Risk Taxonomy</td>
</tr>
<tr>
<td>(Heat Mapping)</td>
<td></td>
<td>- Heat Map</td>
</tr>
<tr>
<td>3-1 Mitigation Planning</td>
<td>Plan for mitigation where a risk level exceed the risk tolerance level</td>
<td>Risk Taxonomy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Mitigation Plan</td>
</tr>
<tr>
<td>3-2 Mitigation Installation</td>
<td>Execute the mitigation plan</td>
<td></td>
</tr>
</tbody>
</table>
Open Risk Universe

Why you need Open Risk Universe

• Starting point to identify “significant risks” to the company
• Support to uncover risks that are prone to be missed
• Free use for OCEG members
An Example of Risk Definition (1/2)

Risk Universe
- External
- Micro Environment
  - Trading Partners
- Procurement Risk

Risk Event
- Risk Scenario 1: The inability to procure required components or raw materials in a stable conditions.
- Risk Scenario 2: Something could hinder the ability of suppliers to provide the Group with a stable supply of required components or raw materials.

Risk Score
- Impact: LEVEL 4
- Likelihood: LEVEL 3

Residual Risk
- LEVEL 3 -> RED

Related Organization
- PROCUREMENT UNIT
- PROCUREMENT UNIT
- PRESIDENT

Risk Owner
- PROCUREMENT UNIT
- PRESIDENT

Existing Control
- Get a production plan and make a procurement plan in view of the production plan for a stable procurement.

Alternative Control
- Keep an alternative supplier for emergencies

Action plan
- Seek an alternative supplier

Heat Map

Mitigation Plan

Mitigating Plan

Risk Taxonomy
An Example of Risk Definition (2/2)

Risk Appetite

- Level 1: $10 to $25 million impact on profitability.
- Level 2: $2.5 to $10 million impact on profitability.
- Level 3: $500,000 to $2.5 million impact on profitability.
- Level 4: < $500,000 impact on profitability.

Likelihood

- Level 1: Less than 1 in ten years
- Level 2: Less than 1 in a year
- Level 3: Greater than 1 in a year, but less than 10 in a year
- Level 4: Greater than 10 in a year, but less than 100 in a year
- Level 5: Greater than 100 in a year

Impact

Risk Level

- Level 1
- Level 2
- Level 3
- Level 4
- Level 5

Tolerance Level

1-1 1-2 1-3 1-4 1-5
2-1 2-2 2-3 2-4 2-5
3-1 3-2 3-3 3-4 3-5
4-1 4-2 4-3 4-4 4-5
5-1 5-2 5-3 5-4 5-5

Risk Tolerance
- Red: need to mitigate quickly
- Orange: plan and mitigate in regular cycle
- Yellow: monitor carefully
- Green: Safe, no special action

Risk Level

Red: need to mitigate quickly
Orange: plan and mitigate in regular cycle
Yellow: monitor carefully
Green: Safe, no special action
Example of Insurance ERM

**Target Risks**

[Quantitative Risks]
- Market Risk (Interest rate, Stock price, R.E., Products, etc.)
- Credit Risk (Debtor, Reinsurer, Security issuer, etc.)
- Insurance Risk
  - Underwriting Risk
  - Loss Reserve Risk, etc.
- Operational Risk

[Qualitative Risks]
- Strategy Risk
- Reputational Risk
- Compliance Risk
- Liquidity Risk

How to integrate Risk Management Process as well as Risk Reporting...
BMM - Regulation Model

Influencer

External Influencer
- Environment
- Technology
- Regulation
- Supplier
- Customer
- Competitor
- Partner

Internal Influencer
- Infrastructure
- Issue
- Assumption
- Corporate Value
- Resource Quality
- Habit
- Management Prerogative
- Stated
- Unstated

More detailed model to “plug in” here

... plus associations with other parts of the BMM
Simplified Model

- Regulation
- Assessment
- Business Process
- Organization Responsibility
- Directive
- Internal Control
- Desired Result
- Business Rule
- Business Policy
- Objective
- Goal

Relationships:
- Regulation is judged in Assessment
- Regulation is step towards Goal
- Business Rule realizes Business Policy
- Business Process is for Desired Result
- Business Process is for Organization Responsibility
- Directive shapes Internal Control
- Internal Control governs Business Process
- Desired Result delivers Business Process
- Objective is step towards Goal
- Objective is basis of Assessment
- Regulation is basis of Objective
Solvency II

• An integrated risk reporting framework

• Solvency II (Sol2) is the biggest ever exercise designed to bring insurers and reinsurers under one regulatory regime

• Solvency II Introduces two major areas of concern or problems
Solvency II Requirements

• Requires each entity to establish MCR using either a standard formula or an internal model
• Requires each entity to manage the risks to which they are exposed and to determine (and report) their own capital needs (ORSA)
• Requires each entity to disclose publicly, key information that is relevant to market participants
The three pillars of Solvency II

The current XBRL taxonomies for Solvency II reporting are:

1. largely addressing the Pillar I requirements.
2. Generating a lot more data that most national insurance supervision have been collecting

Problem #1 Analytics
The three pillars of Solvency II

Under Pillar 2:

1. Each entity must assess and report its Own Risk and Solvency (ORSA)

2. National supervisors must assess the entities ORSA, and the groups ORSA if required.

Problem #2: Consistency of the ORSA Assessments

INTEGRATED RISK AND CAPITAL MANAGEMENT FRAMEWORK
GRC XML and Solvency II

• The Solvency II GRC Extension Taxonomy Addresses Problem # 2,

• Resulting in a Multi-purpose Electronic Risk Framework (MERF)
Input – materials acted upon
Output – testing results, documentation/workpapers, conclusions, opinions...

High-level Information Flow

GRC Data Model

Lines of Business

Solvency II (detail)

Insurance Company

Solvency II (aggregate I1)

Insurance Syndicate

“Reporting” e.g. ORSA

Resource

Evidence data

Solvency II (aggregate I2)

Solvency II (aggregate I3)

EIOPA

EU Systemic Risk Board (ESRB)

FSA

XBRL26 HOSTED BY XBRL IRELAND
Strategic objectives

The Multi-purpose Electronic Risk Framework (MERF) is a comprehensive model that aims to:

• Provide a universal end-to-end solution enabling both risk generators (enterprises) and risk supervisors (regulators) to electronically communicate information about financial sector risks in quality and timely manner
• Enable incorporation of multiple financial and risk reporting, standards and frameworks
• Integration of disparate systems and technologies used by enterprises and regulators
• Facilitate new analysis and supervision models improving the overall systemic risk and integrated supervision of financial markets
• Efficiently combine and address multi-tier information requirements including financial reporting to market and supervisors and reporting of internal risk management, mitigation and control models
Technical objectives

Technical objectives of the Multi-purpose Electronic Risk Framework (MERF) include:

• Consistent, explicit, unique and comprehensive coverage of data models of financial, statistical and risk control and management information
• Linking mechanism between data points from respective data models
• Enable electronic generation, transmission, collection, validation, storage, analysis and publication of relevant information through adoption of XBRL and GRC-XML standards
• Integration with multiple existing XBRL taxonomies
Target users of MERF

Financial sector entities including:
- banks
- credit unions
- insurance and reinsurance bodies
- pension funds
- investment funds
- credit rating agencies
- others

Financial sector supervisors including:
- central banks
- financial services authorities
- banking, insurance and pension funds supervisory commissions
- government agencies
Additional Potential Beneficiaries

• Capital market entities:
  - Investors and analysts
  - Listed companies
  - Data aggregators and publishers

• Academic and research communities
• International standard-setting organizations
• International financial organizations
• Software vendors and developers
Summary

• Federated environments: visibility across silos
• Eliminate or reduce redundancies
• Standardization: XBRL, XBRL GL, GRC-XML, Ontologies
• Integration of different areas:
  - Security risk, IT risk, Financial risk, Operational risk, and others: Many areas, one language
• Continuous monitoring and audit
• Consistency of Regulatory Supervision
• Towards intelligent, predictive, context-aware data management
Enabling transparency and traceability
Thank You!

Questions?