The OMG GRC GRID

High Level Overview

Object Management Group GRC Program

http://www.omg.org/
Introduction

- The Object Management Group was founded in 1989. Today, with over 470 member organizations, OMG is the largest and longest standing not-for-profit, open-membership consortium developing and maintaining computer industry specifications.
- OMG members define standards with a worldwide, neutral, open, accessible and rapid development process that assures freely available specifications with implementations.
- OMG members are currently developing standards in two dozen verticals including:
  - Finance, Healthcare, Business Modeling & Integration, e-Government

OMG Specifications

OMG Relationships

QuickTime™ and a decompressor are needed to see this picture.
### Who are OMG?

<table>
<thead>
<tr>
<th>Adaptive</th>
<th>Credit Suisse</th>
<th>IDS Scheer</th>
<th>NASA</th>
<th>SAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe</td>
<td>Daimler-Chrysler</td>
<td>IONA</td>
<td>NIST</td>
<td>Siemens</td>
</tr>
<tr>
<td>Alcatel</td>
<td>Deere &amp; Co.</td>
<td>Interactive Objects</td>
<td>Nokia</td>
<td>Sun</td>
</tr>
<tr>
<td>ASMG</td>
<td>EDS</td>
<td>Kaiser-Permanente</td>
<td>Northrop</td>
<td>Telefonica</td>
</tr>
<tr>
<td>BAE Systems</td>
<td>Fujitsu</td>
<td>Kennedy Carter</td>
<td>Oracle</td>
<td>Thales</td>
</tr>
<tr>
<td>BEA Systems</td>
<td>General Dynamics</td>
<td>Lockheed Martin</td>
<td>Promia</td>
<td>Toshiba</td>
</tr>
<tr>
<td>Boeing</td>
<td>HP</td>
<td>MedicAlert</td>
<td>PrismTech</td>
<td>Unisys</td>
</tr>
<tr>
<td>CA</td>
<td>Hitachi</td>
<td>Mentor Graphics</td>
<td>Raytheon</td>
<td>VHA</td>
</tr>
<tr>
<td>Cisco</td>
<td>IBM</td>
<td>Motorola</td>
<td>Rockwell</td>
<td>W3C</td>
</tr>
</tbody>
</table>
The OMG and Regulatory Compliance

- OMG Members - mostly global firms - were struggling with regulatory compliance costs and complexities

- OMG reviewed available resources, and determined that a lack of standards for modeling regulations was hindering development of better tools to automate common compliance tasks

- The OMG launched initiatives to address these issues in April 2005
GRC Today: Basic Findings

- Governance issues are becoming pervasive, so identifying and exploiting common enterprise and IT governance best practices will pay increasing dividends;
- Enterprise risk management is emerging as a cross-functional discipline, but progress is hampered by the lack of relevant standards and interoperable tools;
- Regulatory compliance costs IT departments billions of dollars annually;
- Rules are often complex, occasionally in conflict with each other, and always subject to change.
- Competitors within a market typically gain no sustainable advantage through their GRC investments, but divert capital and management resources that could be used to grow their enterprises.
- Failures can cause cascading loss of confidence within a market, so it is to every participant’s advantage to collaborate and share these practices.
- GRC tools should interoperate seamlessly using open specifications for GRC data representation.
The Problem

- Growing number of International, National and Local regulations, standards, policies
- Growing number of conflicts, redundancies, overlaps
- Multiple jurisdictions, conflicts in areas of privacy and security, reporting, etc
- Where does one find guidance on: which ones apply in Canada? When do they apply? What is the impact to a specific sector of the economy? Implementation options?

*The OMG GRID helps address these questions*
The GRID: Goals and Objectives

- Provide the regulatory agencies to provide and publish guidance on the application of specific and interrelated regulations

- Improve the ability of enterprises and government agencies to:
  - Effectively comply and demonstrate compliance with relevant regulations
  - Reduce the time, and initial and on-going costs of complying with regulations

- Improve the ability of vendors of IT based products and services to develop offerings that:
  - comply with regulations, or that
  - enable the planning, implementation and control of processes and rules to comply with regulations
### GRC- GRID Geography Scope

The first release of the GRID is focused on the banking vertical, and includes rules from the following countries:

<table>
<thead>
<tr>
<th>Argentina</th>
<th>Hong Kong</th>
<th>Singapore</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>India</td>
<td>South Korea</td>
</tr>
<tr>
<td>Belgium</td>
<td>Italy</td>
<td>Spain</td>
</tr>
<tr>
<td>Brazil</td>
<td>Japan</td>
<td>Sweden</td>
</tr>
<tr>
<td><strong>Canada</strong></td>
<td>Luxembourg</td>
<td>Switzerland</td>
</tr>
<tr>
<td>China</td>
<td>Mexico</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>France</td>
<td>Netherlands</td>
<td>USA</td>
</tr>
<tr>
<td>Germany</td>
<td>Portugal</td>
<td></td>
</tr>
</tbody>
</table>

and multi-national entities such as the European Union (EU)
Types of Rules Captured

- Outsourcing Regulations / Principles / Guidelines
- IT Governance and Operational Risk (incl. IT risk) Management
- Data Privacy & Transfer
- Spam
- Data Retention & Secrecy
- Security & Safety of IT Systems and Infrastructure
- Business Resiliency (incl. BCP/DRP)
- Electronic Surveillance & Monitoring
- Electronic Transactions & Digital Signatures
- Networks & Firewall Policies.
Global snapshot on privacy laws

Blue---Existing Private Sector Privacy Laws

Red---Emerging privacy Sector Privacy Laws
Privacy in Canada

- CAN SPAM Act
- Canadian Comprehensive Auditing Foundation
- Canadian Public Accountability Board (CPAB)
- Canadian Securities Administrators (CSA) Proposed Multilateral Instrument 52-111
- CanCERT
- DRIE Canada (Disaster Recovery Information Exchange)
- Institute of Chartered Accountants of Ontario
- Multilateral Instrument 52-109 - Ontario Securities Commission
- Multilateral Instrument 52-110: Audit Committees
- PIPEDA (CAN/CSA-Q830-96)
Integrating the GRID with a Policy Management Platform

- Linking Regulatory Requirements to Internal Policy
- Enable the company/Client to comply with regulatory requirements
- Provide traceability and transparency
- Continuous Audit-ability: assess the effectiveness of policies and mitigate risks

Regulations, Frameworks, Guidelines, …

Policies, Corporate Actions, Assessments, Rules, Processes
What do you get out of the Box

- The GRID Framework (can be customized or ready to use as is)
- A starter kit containing a few hundred regulations, guidelines and related industry frameworks
- A strong model based on formal methodology and standards
- A related vocabulary of terms for all Canadian Jurisdiction in one vertical
  Additional jurisdiction and vertical can be added as part of the customization
- An integration Kit to enable the use of GRID in Web-based distributed environments
What do you get to develop

- Extending the GRID to fit your specific requirements
- A taxonomy to classify your regulatory and risk view (supported by the GRID framework)
- Vocabularies, interpretations of relevant regulations to store in the GRID repository
What are the related costs?

- **Initial Costs**
  - Sponsoring and Licensing for the GRID: USD 200k annually
  - Maintenance: free 1st year then 15% a year (includes all GRID upgrades)
  - Hosting: USD 5k per month

- **Estimated Implementation Costs**
  - Customization: USD 25k per month for three months minimum
  - Assuming internal resources available on a part time basis
Thank You!

For any questions, please contact: 
ken@omg.org