Sharing Policy Rules for IT Governance

Adrian Bowles, PhD
Program Director, Governance Risk Management & Compliance Roundtable
www.grcroundtable.org
October 2007

adrian@omg.org
adrian@cosource.net
Sharing IT Governance Policy Rules

- The OMG and GRC
- IT Governance
- Collaborative IP Development as a Business Model
- The GRID
- The GRC-RT ITG Project
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, BMI (business modeling & integration)

OMG Specifications

OMG Relationships

Copyright © 2007 by Adrian Bowles. All Rights Reserved.
# Worldwide Scope

<table>
<thead>
<tr>
<th>88Solutions</th>
<th>Credit Suisse</th>
<th>IDS Scheer</th>
<th>NASA</th>
<th>SAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive</td>
<td>Daimler-Chrysler</td>
<td>IONA</td>
<td>NIST</td>
<td>Siemens</td>
</tr>
<tr>
<td>Adobe</td>
<td>Deere &amp; Co.</td>
<td>Interactive Objects</td>
<td>Nokia</td>
<td>Sun</td>
</tr>
<tr>
<td>Alcatel</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>

![Flags](image)
GRC Today: Basic Findings

- Governance issues are pervasive, so identifying and exploiting common enterprise and IT governance best practices will pay increasing dividends;
- 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.
OMG’s GRC Activities

- **RC-SIG**
  - Established 4/2005
  - Following the OMG process to develop modeling standards to represent regulations, facilitating automation of compliance tasks
  - Met throughout 2005 to identify key requirements for RC modeling
  - Currently preparing RFPs

- **GRC Roundtable (GRC-RT)**
  - Moderated Forums, Events, & Research
  - Global Rules Information Database (GRC-GRID)

- These programs have been supported by IBM, CA, HP, Unisys, Fair Isaac, Pegasystems, Adaptive, Lumigent, InRule and several large user organizations
GRC-Roundtable

The GRC-Roundtable will provide global GRC professionals with:

- **A Moderated Community** – Open and ongoing exchange of information is critical to achieve the goals of the GRC-RT. Electronic and in-person exchange of ideas and experiences is critical, so the GRC-RT provides continuity through online forums complemented by live events held around the world.

- **A Voice** – The GRC-RT is uniquely positioned as a unifying force in the GRC market. It acts as a GRC IP integrator, bringing together the best concepts, mappings, controls and frameworks while exploring the needs and concerns of its members. The GRC-RT will produce and disseminate research findings in the form of webinars, white papers, and events to educate and shape public and government opinion based on the experiences of its members.

- **Resources** - The GRC-RT is developing the *Global Rules Information Database (GRC-GRID)* – an open database of GRC rules, regulations, standards, and government guidance documents, as well as a survey of the regulatory climate around the world.
GRC-Roundtable

The GRC-Roundtable will:

➤ Support leading developers of GRC frameworks and information, including ISACA, IT Governance Institute, IT Compliance Institute, etc. and provide a forum to encourage and enable interoperability of their IP.

➤ Support the OMG’s efforts to develop and disseminate specifications for GRC data representation and capture.

➤ Collaborate with regulators and their affiliates, such as the SEC, PCAOB and National Archives and Records Administration, to encourage the publication of proposed and enacted rules in standard formats to support automated analysis, interpretation, and compliance wherever feasible.

➤ Facilitate the community-oriented development and distribution of common rules for domains of interest to members.
  ➤ The first such set is for IT Governance
What is IT Governance *and why should I care?*

IT Governance (ITG) is

- An emerging discipline
  - focused on managing and improving the delivery of IT through improved alignment with business goals and strategy, value delivery and risk management. ITG supports IT through all aspects of business (from innovation through growth and operations).

- A critical business issue
  - as IT failures rooted in process errors are too common and the resulting loss of revenue, reputation, and opportunity are unacceptable.

- Part of a good corporate governance structure
  - used to help ensure that IT delivers *what* is expected, *when* it is expected.

- An opportunity for business differentiation
  - through delivery of superior IT services.
ITG is Critical Because

IT-Based Competitive Advantage is Fleeting

- Applications can’t differentiate indefinitely.
- Timely delivery of new IT projects and services is critical to sustained growth and profitability.
- ITG offers benefits throughout the lifecycle from concept to code and operations.
Leading Frameworks: Converging IP from Competing Organizations

<table>
<thead>
<tr>
<th>Framework</th>
<th>Source</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ITIL</strong> (IT Infrastructure Library)</td>
<td>Office of Government Commerce (OGC) UK</td>
<td>OGC is an organization whose mission is to generate revenue for the UK Treasury via book and online access sales and accreditation revenue (through third parties TSO and APMG).</td>
</tr>
<tr>
<td><strong>COBIT</strong> (Control OBjectives for IT)</td>
<td>IT Governance Institute (Affiliate of ISACA)</td>
<td>Professional association whose mission is to provide benefit to members. IP developed by membership and ITGI staff. Focused on management controls, management practices, governance, closely aligned with Sarbanes Oxley requirements. Member benefits to advance ISACA/ITGI organization value.</td>
</tr>
<tr>
<td><strong>ISO 20000</strong> (IT Service Management Standard)</td>
<td>ISO IEC – international standards body – members are national standards bodies.</td>
<td>International standard. Overlapping management system and certification standard with 9001 – some confusion in standards as a result. There is a related for-profit certification scheme. Certification is not part of the standard.</td>
</tr>
</tbody>
</table>
Areas of overlap will continue to expand as individual frameworks evolve.
Complete convergence won’t happen.
Although mappings/cross references between the frameworks are becoming available, it is left as an exercise for the end-user to put it all together.
It is in the best interest of the framework developers to get users to adopt everything from their framework, and add differentiated practices from others as necessary - this is not necessarily in the best interest of the user.
Best approach will be to adopt and integrate policies representing the best/most relevant practices from each, but avoid lock-in to any one of them.
Frameworks are Business Focused

These frameworks address key business objectives of improving service delivery and operations, but the leaders come from different backgrounds.

- COBIT reflects business concerns in IT (Driven largely by governance regulations like Sarbanes Oxley Act)
- ITIL & ISO 20000 reflect IT concerns in business (Need to overcome traditional IT process weaknesses and lack of predictable results)

- All are currently being updated
- All are becoming more business-focused
  - As IT becomes more integrated into business processes
  - As increasing regulatory constraints impinge on IT management and operations
ITG Has a Role Throughout the BUSINESS Lifecycle

The Business Lifecycle: From Vision to Value

1. Context Analysis Intelligence
   - Identify Requirements
   - Identify & Model Current Processes

2. Opportunity Identification
   - Identify & Model Alternatives
   - Evaluate Alternatives

3. Opportunity Evaluation/Selection
   - Construct Components and Aggregates
   - Identify & Acquire Packages, Frameworks/Components

4. Execution
   - Integration & Operation
   - Integration, Execution, Refinement

- Traditionally, IT has been seen in a supporting role (“aligned” with business objectives).
- These frameworks were developed to map to the Execution Quadrant in this Business Lifecycle model.
- Going forward, IT must be integrated into the business lifecycle, with services that support all phases of business-value delivery.
Focus Where Customers Notice

Own/Innovate

Buy/Collaborate

Value Adding Applications

Infrastructure

Visible Excellence

Visible Failures

Copyright © 2007 by Adrian Bowles. All Rights Reserved.
Control vs Share Strategy

- Wasted Resources
  - Application Portfolio
  - Business Rules
- Optimal Allocation
  - Share
  - Missed Opportunities
- Control
The Great Roll-Up

Aggregation: Who has the big picture Vs who needs it?

Issues

- Data quality
  - Consistent
  - Current
  - Complete
Business Runs on Rules
Characteristics of Change

Rate of Change vs. Cost of Change

- High Rate of Change
- Low Rate of Change

- Low Cost of Change
- High Cost of Change

- Data
- Business Logic
- Infrastructure

- Fashion
- Culture

- Pricing
- New Market Entry
Automating GRC & IT Governance

Goal: Automated Detection of New Regulatory Requirements and Rule-Based Generation of Policies

Query: SIC/NAICS, Geography…

Repository of Global Regulations

IT Strategy & Operations

IT Compliance Policies/Procedures

Relevant Regulations

Updates

Gap Analysis

Relevant Regulations

Vendors

Users

Auditors

Other Stake-holders

Regulators

Rules

Goals:

- Automated Detection of New Regulatory Requirements
- Rule-Based Generation of Policies
**HIPAA**

164.308(a)(6)(ii) Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, and document security incidents and their outcomes.

164.310(d)(i) Disposal Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

164.308(a)(5)(ii)(ii)(b) Protection from malicious software [In deciding which security measures to use, a covered entity must take into account the following factors:] Procedures for guarding against, detecting, and reporting malicious software.

**SOX**

404(a)(2) [The Commission shall prescribe rules requiring each annual report... to contain an internal control report, which shall... contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.]

**CobIT**

DS 5.7 Security Surveillance IT security administration should ensure that security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally, and is acted upon in a timely manner.

DS 11.20 Retention Periods and Storage Terms Retention periods and storage terms should be defined for documents, data, programs and reports and messages (incoming and outgoing)...

DS5.19 Malicious Software Prevention, Detection and Correction Regarding malicious software, such as computer viruses or Trojan horses, management should establish a framework of adequate preventative, detective and corrective control measures, and occurrence response and reporting.

**ITIL, ISO 17799...**

**Networks are monitored for security threats**

**Business records are archived.**

**Security events are logged**

**Records are destroyed in accordance with the retention policy.**

**Anti-virus software is up to date**

**Anti-virus software is running**

**Anti-virus software is installed**

---

Capturing Complex Mapping Relationships

*Copyright © 2007 by Adrian Bowles. All Rights Reserved.*
The Design Was Collaborative...
Implementation and Operations are Collaborative, Too.

Already received compliance and privacy data on over 100 countries from individuals, top tier banks and brokerage firms.
The GRC-RT ITG Project

Goals - Identify/build a common set of ITG Policies with broad applicability, and make them available via the GRID

- Participation is open to all GRC-RT members
- Cultural Challenges - Some firms exhibit NIH syndrome
- Technical Challenges
- Benefits
  - Reduced Cost
  - Reduced Risk
  - Better Coverage and Currency
Supporting Shared IT Governance Practices
The GRC-RT ITG Project

Status

- New Initiative
- Forum to be launched in December 2007 at www.grcroundtable.org
- Kickoff meeting to be held in Q1 2008
- Ready to share IP with individual firms and associations now.
- First step will be to identify all relevant frameworks and existing overlaps and mappings.
Sharing Policy Rules for IT Governance

Adrian Bowles, PhD
Program Director, Governance Risk Management & Compliance Roundtable
October 2007