18th International XBRL Conference

Governance, Risk, and Compliance: Panel Session

Lane Leskela – OCEG
Scott Mitchell – OCEG
Scott C. Rosenfelder – Deloitte & Touche LLP
Panel Session Agenda

We will provide you with:
1) Overview of GRC
2) Presentation from OCEG on compliance and ethics focusing on the use of technology
3) Utilizing XBRL for Internal Control tagging and monitoring
4) Open Panel Discussions
Governance, Risk, and Compliance
Governance, Risk, and Compliance (GRC)

- GRC refers to taking an integrated, enterprise-wide approach to Governance, Risk Management, and Compliance:
  - **Governance** – The Board of Directors’ and management’s structures, policies, processes, and controls that focus on long-term value through the ethical, equitable, efficient, and effective operation of the business
  
  - **Risk Management** – An organization’s systematic process to identify, assess, manage, and monitor upside and downside risks to the business
  
  - **Compliance** – An organization’s process to demonstrate its employees and agents adherence to policies and procedures, laws, and regulations

- GRC is transformational and addresses the people, process, and technology enhancements required to achieve risk intelligence
Current State

- The “universe” of risks, regulations, and compliance requirements continues to expand at an increasing rate.

- Market, regulatory, and legal tolerance for failures continues to decrease.

- Enterprise governance, risk management, and compliance activities are highly fragmented:
  - Have evolved over time from the bottom up, often in reaction to “breakdowns” or new regulations.
  - Highly expensive, but few have true handle on cost.
Risk Ignorance

CURRENT STATE
In some organizations, the current state of governance, risk and compliance processes is disorganized, unnecessarily complex and fragmented.

- Organizational & functional silos
- Lack of visibility
- Poor integration
- Duplication
- Slipping through the cracks
- Complexity
- Fragmentation
- High costs
- Wasted information
- Wasted resources
- Vulnerability
- Unnecessary complexity and inflexible

(c) OCEG, 2008
Risk Intelligence and Integrated GRC

XBRL enhances reporting transparency by using publicly developed taxonomies.

XBRL can facilitate data exchange by using open standards.

XBRL enables SOA architectures for interoperability.
Open Compliance and Ethics Group
What is OCEG?

OCEG is the leading nonprofit that helps organizations drive principled performance™ with a global community of skilled practitioners focused on improving governance, risk management, and compliance processes.

- **Guidelines and Standards – what should we do?**
  - Process standards (key concepts, components, and terminology)
  - Technical standards (key systems and integration points)
  - DEVELOPED by experts and PUBLICLY vetted to ensure quality

- **Evaluation Criteria and Metrics – how are we doing?**
  - Effectiveness and performance evaluation (suitable criteria)
  - Reporting and disclosure guidance
  - Tools and technologies to appropriately benchmark

- **Community of Practice – how/what is everyone else doing?**
  - Discover, create, and evolve guidelines
  - Use online tools and resources
  - Collaborate with peers in a NUMBER of professions

OCEG has over 15,000 members in 46 countries representing 66 GRC disciplines.
Mission: The Integration of Disciplines

OCEG brings together disciplines and professions to collaborate and pursue a common mission: to refine and improve the practice of GRC

- Governance
- Risk Management
- Compliance/Legal Management
- Human Capital Management
- Change Management
- Ethics Management
- Internal Audit
- Security
- Quality Management
- Project Management
- Information Technology
- Financial and Resource Planning

 XBRL eXtensible Business Reporting Language
Elements of the OCEG GRC Capability Model

**MONITOR AND MEASURE**
- M1 – Context Monitoring
- M2 – Performance Monitoring and Evaluation
- M3 – Systemic Improvement
- M4 – Assurance

**CONTEXT AND CULTURE**
- C1 – External Business Context
- C2 – Internal Business Context
- C3 – Culture
- C4 – Values and Objectives

**ORGANIZE AND OVERSEE**
- O1 – Outcomes and Commitment
- O2 – Roles and Responsibilities
- O3 – Approach and Accountability

**RESPOND AND RESOLVE**
- R1 – Internal Review and Investigation
- R2 – Third-Party Inquiries and Investigations
- R3 – Crisis Response and Recovery
- R4 – Remediation and Discipline

**INFORM AND INTEGRATE**
- I1 – Information Management and Documentation
- I2 – Internal and External Communication
- I3 – Technology and Infrastructure

**DETECT AND DISCERN**
- D1 – Hotline and Notification
- D2 – Inquiry and Survey
- D3 – Detective Controls

**ASSESS AND ALIGN**
- A1 – Risk Identification
- A2 – Risk Analysis
- A3 – Risk Optimization

**PREVENT AND PROMOTE**
- P1 – Codes of Conduct
- P2 – Policies
- P3 – Preventive Process Controls
- P4 – Awareness and Education
- P5 – Human Capital Incentives
- P6 – Human Capital Controls
- P7 – Stakeholder Relations and Requirements
- P8 – Preventive Technology Controls
- P9 – Preventive Physical Controls
- P10 – Risk Financing/Insurance

(c) OCEG, 2008
The OCEG Technology Council was formed to help address strategic, operational and technical issues that professionals face when applying Information Technology (IT) to governance, risk management, compliance (GRC) and ethics management.

Technology Council members meet monthly in specialized working groups focused on GRC technology architecture, standards, and implementation tools. These Work Groups include the GRC Blueprint™, GRC Roadmap™, and GRC-XML™ programs.

The entire council convenes quarterly to review the progress of the individual working groups, discuss key issues facing GRC professionals, and to identify new GRC technology alignment programs for OCEG.

The OCEG Technology Council engages 37 of the world's leading GRC software, services, and content providers and user organizations in the development of strategic and technical resources that help IT and business professionals improve the practice of GRC within their organizations.
OCEG Technology Council Members
The OCEG GRC Integrated Technology Model

Industry-Specific Requirements

Industry Process Applications

GRC Management Requirements

GRC Core Applications

Business Applications

Technology Infrastructure

Business Requirement

IT Delivery

Internal and External Content Specialists
(e.g., law firms, consultants, departmental staff, directors, managers)

Role and Context Applications
(e.g., compliance processes and reporting; risk, quality, audit, legal, and contract management)

Organizational Functionality
(e.g., ECM, BPM, BI, LMS, ERP)

IT infrastructure
(e.g., identity management, Databases, Information Security)
Member A Case:
GRC-XML (XBRL) Components (Case Management)

1. Supporting interchange of help line data from content providers for this domain
2. Supporting interchange of current case management data
3. Supporting interchange of education status (i.e. courses taken by employees to mitigate risk)
   A. (1) and (2) are ways of communicating the result of an incident
   B. (1) and (2) demand a unified solution so that a help line incident shares as much structure with a case management incident as possible
   C. For (1) and (2) we are leveraging and extending taxonomy in the following domains:
      I. Data Security
      II. Risk classification
      III. Performance-based controls
      IV. Message Processing
      V. Geographical Location
      VI. User identity
      VII. Data Privacy
   D. Area (3) is necessary to communicate actions taken to prevent incidents
**Member B Case:**
GRC-XML (XBRL) Components (Controls)

1. **Identification of business control point(s)**
   - A. Process, sub-process, control name, and ID
   - B. Financial account(s) impacted
   - C. Process owner details (name, address, business unit …)

2. **Risk assessment**
   - A. ID, business risk(s) addressed by the control point, other mitigating controls
     1. Approval, version, effective date
     2. Related file attachments

3. **Control testing activities**
   - A. Test plans (header-level)
     1. ID, objectives, budget, person responsible
     2. Approval, version, effective date
     3. Related file attachments
   - B. Tests (detail)
     1. ID, objectives addressed, test type, selection method, source population details, test procedure
     2. Approval, version, effective date
     3. Related file attachments
Member B Case:
GRC-XML (XBRL) Components (Continued)

4. Exceptions (related to one or many detail tests)
   A. ID, description, owner, reviewed, resolution (plan), resolution (actual), status
      I. Approval, version, effective date
      II. Related file attachments

5. Control deficiencies (related to one or many detail tests, related to one or many control points)
   A. ID, description, found by test(s), impacts control(s), severity, category
      I. Approval, version, effective date
      II. Related file attachments

6. Control point assessment
   A. ID, operating effectiveness (pass/conditional pass/fail), evidenced by control deficiencies, resolution (plan), resolution (actual)
      I. Approval, version, effective date
      II. Related file attachments
   B. Operational information which may impact the assessment (for example, whistle-blower reports) – According to Member A’s taxonomy for incidents
   C. Vendor applications will manage specific test plans, as XBRL governs common criteria, standardized control language for incidents, defines related control values
OCEG GRC-XML (XBRL) Program Management Process

- **OCEG**
  - Owns the initiative
  - Is an official member of XBRL International
  - Provides “vision” and program governance
  - Promotes final schema adoption

- **Technology Council - Jurisdiction**
  - Encourages Member Contributions and Participation
  - Drives the production schedule
  - Provides the Work Group Members
  - Provides technology, technical skills, and methodology

- **Work Group – Steering Committee**
  - Executes the development methodology
  - Develops and reviews all deliverables
  - Builds schema consensus
  - Creates and delivers the Business Object Documents
Proof of Concept: Internal Control and XBRL
Beyond Financial Reporting

- Exploring Taxonomy Development:
  - Global Ledger
    - Captures accounting system information (Journal Entries, Trial balance, Vendor/Employee/Customer data).
    - SRCD (Summary Reporting Contextual Document) provides mechanism for linking accounting system detail to reporting taxonomies.
  - Internal Control
    - Proof of concept using XBRL to document Internal Control structure and assessments. Initial work done by representatives of large accounting firms.
    - IFRS, FINREP, COREP, etc.
- Integration of Disparate Systems and Data
- XForms – A User Interface for XBRL
  - XForms is a standard from W3C, allows creation of sophisticated user interfaces for XBRL documents.
Proof of Concept Objectives

- Validated the ability to create a XBRL Internal Control taxonomy based of Deloitte’s Risk and Control Knowledgebase (RACK)

- Validated ability to convert general ledger (GL) data from SAP and Oracle into XBRL GL instance documents

- Validated ability and value of combining XBRL GL, XBRL Internal Control, and XBRL FR instance documents for enhanced reporting:
  - Financial Statement → Internal Control and Assessment Detail
  - Financial Statement → GL Transaction Detail
Internal Control Taxonomy

- Explored opportunities and value of a taxonomy built for the purpose of reporting on Internal Controls:
  - XBRL Internal Control Taxonomy
    - Taxonomy comprised of processes, subprocesses, objectives, risks, and controls defined in a standard taxonomy
    - Utilizing dimensionality for entity uniqueness
    - Taxonomy populated with Deloitte RACK data – a proprietary set of internal control frameworks organized by Industry and Business Processes
Integration Proof of Concept – Technical Overview

**Source Systems**
- SAP: XBRL Adapter
- ORACLE: XBRL Adapter
- Other Source Systems: XBRL Adapter, Web Services

**XBRL Repository**
- Global Ledger
- FR Taxonomies and Instance Documents
- Internal Control Taxonomies and Instance Documents

**Enterprise Taxonomy Management**

**Enterprise Reporting and Search**
- CFO Dashboard
- Enterprise Search
- Financial Statements

**XBRL Adapters/Web Services**
- Periodic pull of general ledger information from source systems and stored in summarized format
- Additional data can be extracted on queries executed if needed by ORACLE taxonomy for control monitoring purposes
- Other sources could include Microsoft Excel or other Internal/Control and Testing Data source systems

**XBRL Repository**
- Central repository for all enterprise XBRL taxonomies and instance documents
- Historical record of extracts allows for performance and trend reporting

**CFO Dashboard**
- Financial Performance and Compliance views
### CFO Dashboard

**Financial Statement**

<table>
<thead>
<tr>
<th>ABC Corp</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Balance Sheet</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assets</td>
<td>4,500,000</td>
<td>4,750,000</td>
<td>5,000,000</td>
</tr>
<tr>
<td>Current Assets</td>
<td>2,000,000</td>
<td>2,250,000</td>
<td>2,500,000</td>
</tr>
<tr>
<td>Quick Assets</td>
<td>360,000</td>
<td>410,000</td>
<td>460,000</td>
</tr>
<tr>
<td>Cash and Deposits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash On Hand</td>
<td>125,000</td>
<td>150,000</td>
<td>175,000</td>
</tr>
<tr>
<td>Deposits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Checking Accounts</td>
<td>150,000</td>
<td>160,000</td>
<td><strong>170,000</strong></td>
</tr>
<tr>
<td>Ordinary Deposit</td>
<td>1,000</td>
<td>1,100</td>
<td>1,200</td>
</tr>
<tr>
<td>Other Current Deposit</td>
<td>25,000</td>
<td>35,000</td>
<td>45,000</td>
</tr>
<tr>
<td>Time Deposit</td>
<td>5,000</td>
<td>4,000</td>
<td>3,000</td>
</tr>
<tr>
<td>Notes Receivable and Accounts Receivable, Trade, Net</td>
<td>1,500,000</td>
<td>1,600,000</td>
<td>1,700,000</td>
</tr>
<tr>
<td>Notes Receivable, Net</td>
<td>25,000</td>
<td>45,000</td>
<td>65,000</td>
</tr>
</tbody>
</table>

**XBRL FR**

Standard framework / definition for an organization
### CFO Dashboard

**Financial Statement > Global Ledger Detail**

<table>
<thead>
<tr>
<th>Acct #</th>
<th>Acct Description</th>
<th>Acct Type</th>
<th>Sub-Acct #</th>
<th>Sub-Acct Description</th>
<th>Sub-Acct Type</th>
<th>Amount</th>
<th>Debit / Credit</th>
<th>Post Date</th>
<th>Source System</th>
<th>Post Status</th>
<th>ID #</th>
<th>ID Desc.</th>
<th>ID Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>Accounts Payable</td>
<td>Acct</td>
<td>000</td>
<td>Corporate</td>
<td>Dept</td>
<td>100,000</td>
<td>Credit</td>
<td>2007-02-15</td>
<td>SAP</td>
<td>P</td>
<td>0100</td>
<td>John Smith</td>
<td>Customer</td>
</tr>
<tr>
<td>1000</td>
<td>Accounts Payable</td>
<td>Acct</td>
<td>010</td>
<td>APAC</td>
<td>Dept</td>
<td>50,000</td>
<td>Credit</td>
<td>2007-02-16</td>
<td>SAP</td>
<td>P</td>
<td>0100</td>
<td>John Smith</td>
<td>Customer</td>
</tr>
<tr>
<td>1000</td>
<td>Accounts Payable</td>
<td>Acct</td>
<td>020</td>
<td>EMEA</td>
<td>Dept</td>
<td>20,000</td>
<td>Credit</td>
<td>2007-02-17</td>
<td>Oracle</td>
<td>P</td>
<td>0300</td>
<td>Tom Jones</td>
<td>Customer</td>
</tr>
</tbody>
</table>

---

**XBRL GL**

Allows mapping of financial account to source transaction data
<table>
<thead>
<tr>
<th>Entity</th>
<th>Rpt Period</th>
<th>Process</th>
<th>Sub-Process</th>
<th>Control Objective</th>
<th>Assertion</th>
<th>Control Objective Rating</th>
<th>Control Activity</th>
<th>Control Activity Response</th>
<th>Assessor</th>
<th>Reviewer</th>
<th>Assessment Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC Corp</td>
<td>2007-Q2</td>
<td>Procure Materials and Services</td>
<td>Payment Process</td>
<td>Credit notes and other adjustments are accurately calculated and recorded.</td>
<td>Recording</td>
<td>Minor Gaps Identified</td>
<td>Statements received from suppliers are reconciled...</td>
<td>No</td>
<td>Steve Johnson</td>
<td>Tom Jones</td>
<td>Review</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Diebursement s are recorded in the period in which they are issued.</td>
<td>Cut off</td>
<td>Meets Guidance</td>
<td>Diebursement s at, before, or after the end of an a...</td>
<td>Yea</td>
<td>John Williams</td>
<td>Tom Jones</td>
<td>Closed</td>
</tr>
</tbody>
</table>

XBRL IC Ties financial accounts to controls
Open Panel Discussions
GRC Goals and XBRL Benefits

GRC goals closely align with potential benefits provided by XBRL

**GRC Goals**
- Streamlined business processes and data elements
- Integration – Seamless data exchange between and among compliance initiatives
- Transparency and visibility
- Standardization of compliance structures, data elements
- Reduced costs

**XBRL Benefits**
- Cost savings, efficiency, and improved accuracy and reliability
  - Transparency
- Enhanced business reporting and standardization
  - Paperless environment
  - SOA architecture for interoperability

**Improved Risk and Compliance Monitoring**
Open Panel Discussion

- What are the opportunities for enabling for Continuous Control Monitoring and Automated Control Testing with XBRL?
  - What are the value drivers?
- Internal Control Taxonomy Development
  - What is the value of developing, implementing?
- What impact can XBRL make to standardized reporting?
- How will XBRL effect business planning?
- Enterprise Risk Management
  - Have you seen adoption or use of XBRL and ERM/ORM from vendors you are working with?