OCEG®

GRC-XML™

A Common Language for Risk and Controls

Version 1.0
October 2009

The continuing work of OCEG is made possible in part by the generosity of the following organizations. Please join us in thanking these leading organizations and their representatives:

Charter Members/Leadership Council:

Leadership Council:

The purpose of this whitepaper is to provide a high level overview of the GRC-XML initiative, which has been undertaken to develop a standard and common language for the representation, sharing, and processing of Risk and Controls through the establishment of GRC Taxonomy based on XBRL and XBRL GL. The need for a common controls and risk language is present within a single organization as well as between an organization and its external auditors, government regulators, industry associations, and business partners.

This paper discusses the business case and why we need such a standard, as well as the target audience.

Author: Said Tabet may be contacted at stabet@oceg.org

OVERVIEW

The Open Compliance and Ethics Group (OCEG) is a not-for-profit think tank that enables organizations to drive performance and enhance their corporate culture by integrating Governance, Risk Management, and Compliance (GRC) processes via guidelines and standards, evaluation criteria and benchmarks, and a global community of practice.

A working group of OCEG is the OCEG Technology Council. The OCEG Technology Council was formed to help address the strategic, operational and technical issues that professionals face when applying Information Technology (IT) to GRC and ethics management. The OCEG Technology Council has established a provisional XBRL jurisdiction following strong interest in the use of XBRL by OCEG members and adoption by the Technology Council's GRC-XML Initiative working group.

This paper introduces the business case for GRC-XML and the approach taken by the OCEG GRC-XML Working Group to deliver this standard as a common language for Risk and Controls. GRC-XML will serve as the core specification on top of which various extensions may be built.

1. THE PROBLEM

Organizations that are implementing an integrated approach to governance, risk, and compliance or those trying to optimize an individual assurance process discipline face a common challenge in the area of integrating and exchanging data. The efficient exchange of electronic data is not a problem unique to GRC. There are literally hundreds of ways to exchange electronic information, and that is actually part of the problem: having to be familiar with lots of different ways, having to use one way to exchange information with one organization, and a different way to exchange information with another organization. XBRL or any other set of standards to exchange information is not a new concept. It is clear that businesses exchange information and that to effectively exchange information there has to be some level of agreement on how information is exchanged.

At its most basic level, all managers and departments within an organization need a consistent way to measure and communicate controls and risk. If the sales department measures controls and risks differently from the finance or marketing departments, then the corporate executives and board will have a difficult time in accurately assessing the health of the business. This need for standardization only grows as the size and scope of a business grows. Large global organizations such as Siemens, United Technologies, and General Electric

all consist of multiple businesses. The requirement for a consistent means for measuring risk and controls across all their business units is critical for accurately managing and growing these businesses. For example, Siemens has 15 different divisions spanning four different industries (energy, healthcare, consumer products and industrial solutions). Siemens has been working to standardize their internal audit and control procedures across businesses as a means for streamlining costs and efficiencies as well as improving the operational efficiency of their companies. The need for standardization also exists in smaller less complex organizations.

As it relates to information on risk and controls, there are common risk and control models utilized by many organizations – each with their own translation of that model. Take the COSO control model for example. Hundreds if not thousands of organizations utilize the COSO control model to support their Sarbanes-Oxley and other compliance initiatives. However, there is no common, agreed upon, electronic representation of that control model or standardized taxonomy or syntax of the specific controls. Without standardization, the current state is that:

- Within an individual company, different divisions, departments, or assurance groups may be utilizing similar controls but each calling them something different. This minimizes transparency and the ability to aggregate information across the organization
- There is no easy way to compare or benchmark control information between companies
- There is no standardized way for point solutions that support the GRC business processes (internal audit, risk management, compliance, IT GRC, CCM, policy management) to easily communicate information regarding risk and controls

GRC-XML has the potential to:

- Provide the basis for a corporation to standardize on a common language of risk and control
- Provide the ability to compare the results of risk and control initiatives between companies
- Provide the ability for a corporation to integrate information between various GRC systems.

2. SCENARIOS

The market encompasses a broad spectrum of unique systems and solutions to address all aspects of an organization including its people, facilities, IT infrastructure, business applications, corporate responsibilities, legal, regulatory and financial obligations. One of the goals of the GRC-XML program is to enable these disparate systems to share and leverage information efficiently without compromising accuracy and functionality.

One relevant example for the need for a common risk and control language is linking information between the systems that document and report on controls with the systems that monitor and test the effectiveness of those controls. Testing and monitoring is spread across a variety of systems spanning the enterprise business applications (ERP, CRM, SCM, financial, HR, etc.) and IT infrastructure (DB's, operating systems, networks, email, communications, etc.) each with their own technology, methodology and data formats. Consolidating and normalizing this disparate information today is largely a paper exercise with a few exceptions where vendors and customers have collaborated to build some level of integration. The GRC XML initiative would enable these systems to produce and share information more directly. GRC XML would also allow consolidated control management information to be easily shared and leveraged by risk management systems so there could be a seamless flow of risk and control information from the source systems to the corporate dashboard and report.

Another example of the need for leveraging a common language is evident today in how an external auditor interacts with a business to perform an annual IT and financial audit. It's the auditor's job to independently attest to the accuracy of the financial results and the effectiveness of the key controls that underlie the financial systems and processes. To achieve that, auditors are often required to obtain large amounts of raw data and review voluminous documentation and policy manuals. The auditors are required to get all the information they need in a format they can work with before they can begin to analyze and assess the results. This process involves multiple iterations between the auditor and the customer to clarify and explain. If a common language existed, large efficiencies could be attained for both the auditor and auditee in conducting the annual audit.

As described above, the need for a common controls and risk language is present within a single organization as well as between an organization and external organizations such as its external auditor, government regulators, industry associations and business partners.

3. APPROACH

The OCEG GRC-XML approach involves the reuse of existing standards and expressing common practice in a common fashion through agreement on its representation with XBRL. Where XBRL recommendations exist, they are incorporated; where other frameworks or agreements exist, they are represented with XBRL. This enables a standardized flow of more readily shareable and consumable information, starting with XBRL's Global Ledger Framework (XBRL GL), as the standardized payload for data and evidence; moving on to common representations of risks, controls and tests leveraging popular frameworks; and linking on to end reporting using appropriate XBRL taxonomies such as US GAAP and IFRS

3.1 Common definition and expression

OCEG GRC-XML uses the XBRL Specification[1] as the basis for its definitions, validation and communication. Using a single specification promotes consistency, facilitates the use of existing tooling in developing and later working with deliverables, and leverages the experiences of others. Using the XBRL Specification means leveraging a Specification that has been developed over a ten-year period specializing in integrated business reporting. The XBRL Specification lays out the syntax and semantics of taxonomies (where shared codes, definitions and descriptions are maintained and communicated) and instances (where company data, described with the codes from the taxonomies are communicated). As the underlying evidence and eventual reporting is XBRL-based, it is logical to try to use XBRL for the risks, controls and tests that bring that evidence and reporting together.

One of the most important aspects of adopting the XBRL Specification is the strong focus on extensibility. While there are other Specifications useful for defining documents, few formalize the methods of extending and modifying the definitions. XBRL provides the guidance and formalization for allowing users of GRC-XML to customize it for their specific internal needs.

3.2 Data and evidence

Testing of controls requires evidence. XBRL's Global Ledger Framework[2] (XBRL GL) is an existing global, holistic, generic Recommendation from XBRL International that represents underlying details that flow from incoming transactions, through operational, business and accounting systems, and link to end reporting. Rather than create evidence/payload representations from scratch, or attempt to create an inventory of all of the possible evidence standards that are available in the marketplace, we have chosen to leverage

[1] http://www.xbrl.org/Specification/XBRL-RECOMMENDATION-2003-12-31+Corrected-Errata-2008-07-02.htm
[2] http://www.xbrl.org/GLTaxonomy

XBRL GL to represent ERP detail and other necessary representations for the evidence used against which tests are run as well as the associated detailed results of testing.

3.3 Risks, Tests and other Results

The prototype uses XBRL taxonomies to capture and formalize the COSO[3] Enterprise Risk Management Framework (COSO). We have extended the information provided by COSO for capturing test information at a consortium level and illustrated corporate specific extensions as well.

While the prototype illustrates the use of COSO, there are other frameworks adopted in the marketplace, such as COBIT, ISO 31000, or PCI. Any of these frameworks can be used in conjunction with or replacing the prototype COSO framework by developing appropriate XBRL-compliant taxonomies representing their components. GRC-XML will be designed in a modular fashion to facilitate extensions and modifications.

3.4 Benefits

We believe a primary benefit of this approach will be a high return on investment (ROI) of the GRC-XML approach over proprietary approaches. Leveraging existing data representation standards and risk management methodologies should bring the benefit of readily available tools, education and other resources, including employees and consultants with existing skills and knowledge. A standards-based approach should bring the benefits of increased scalability and agility. An extensible approach brings standardized customization, the ability to customize the work of GRC-XML to local business environments with a minimum of compromise.

4. WHO IS INVOLVED

The GRC-XML initiative is backed by the OCEG Technology Council following strong interest from our member organizations. The current working group, headed by Said Tabet, is comprised of professionals representing Approva, Thomson Reuters, Fujitsu, Telos and PricewaterhouseCoopers. The OCEG GRC-XML working group welcomes participation from vendors, user companies, and other organizations and government agencies.

[3] http://www.coso.org


OCEG®
DRIVING PRINCIPLED PERFORMANCE®
Shipper
ShipperKey
ShipperID
ShipperName
Product
ProductKey
ProductID
CategoryID
Price
ProductCategory
Sales
TimeKey
ShipperKey
ProductKey
ItemFreigh
ItemQuani
ItemAll
Discount
Action
Employee
www.oceg.org