Chapter 35
Emerging Standards and Protocols for Governance, Risk, and Compliance Management

Marcus Spies  
LMU University of Munich, Germany

Said Tabet  
EMC Corporation, USA

ABSTRACT
Effective Governance, Risk, and Compliance Management (GRC) software tools and software services need standards – for reasons of technical interoperability as well as reviewing, reporting, and auditing purposes. This chapter introduces an emerging standard for GRC metadata and metadata exchange, GRC-XML, on the background of standard frameworks for IT governance and risk management. This specification is then further analyzed with regard to its integration capabilities into the Object Management Group’s GRC related standards covering business motivation, management of regulation and compliance, business vocabularies, policies, and rules. Finally, the authors discuss in more detail the challenges to business rules applications and automated inferencing when governance, risk, and compliance issues need to be verified in practice.

INTRODUCTION
Governance, Risk and Compliance Management (GRC) is a topic of increasing importance to enterprise software and electronic business technologies. Due to the ever-increasing number and complexity of regulations in all areas of e-business, even basic business interactions need to be engineered for GRC. Appropriate Governance, Risk and Compliance Management needs to be rooted in the overall management of an organization.

With the Open Compliance and Ethics Group (OCEG), a global standardization organization has been formed to define a generic GRC
Emerging Standards and Protocols for Governance, Risk, and Compliance Management

capability model. The industry and public administration member base of OCEG covers key players in many industries, comprising leading global GRC consultancies and software vendors. The OCEG GRC capability model defines key process / management components and outcome areas. Components are further subdivided into elements specifying a key process area for the component together with principles, common sources of failure and recommended practices. Practices are again detailed by key deliverables and enabling technologies. OCEG provides the GRC capability model as a structured document (Mitchell & Switzer, 2009b) and as an assessment data template that provides a framework for specific GRC maturity assessments for OCEG member or customer organizations (Mitchell & Switzer, 2009a).

For governance, the continuous auditing methods and continuous monitoring environments require enterprise software and e-business applications to supply a continuous stream of relevant data as well as control interfaces that allow for agile adaptation and reconfiguration of e-business services. Analogously, risk management in a continuous monitoring environment requires the availability of loss event data on a short-term basis for fast re-estimations and real-time assessments of risks. In financial services, the typical re-estimation period for loans has changed from 1 month to 1 day, which implies the need for massively parallel computations and appropriate infrastructures (Prätzas & Deutsche Bank Finance IT – dbArtos Team, 2010).

The biggest impact of GRC related business transformations, however, can be seen in compliance management. As an example, take the Basel II / Basel III regulations on capital adequacy in the finance sector (Basel Committee on Banking Supervision, 2006). These regulations are set up in a sufficiently general form to allow covering a wide variety of banking services, solutions and regional or national specific conditions. This leaves individual banking services providers with the task to interpret regulatory requirements and define appropriate measurement and control systems that demonstrably guarantee implementation of regulatory compliance. In the Basel II / III framework, for instance, banks can qualify for a certification allowing them to report on the basis of internal measurements (advanced internal measurements approach AIM) instead of being assessed by external evaluators. Therefore, business regulations are not simply collections of business policies or business rules that need to be acted on by an individual business. Instead, these regulations require transformation to and re-definition within the specific business context and demonstrable implementation of the resulting business policies and business rules.

Problem Statement

This transformation to and re-definition process of regulatory and other GRC related requirements into business specific policies and rules needs a modelling framework and supporting technical infrastructure. One candidate framework is the model driven architecture (MDA) proposed by the Object Management Group OMG together with suitable business model specifications, among which the business motivation model or BMM, see (Object Management Group, 2010a), the semantics of business vocabularies and business rules or SBVR, see (Object Management Group, 2008) are most important for GRC. Basing policies and rules definitions on this kind of framework enables intelligent regulatory compliance (Spies, Schacher, & Gubser, 2010). As a real example, KnowGravity, a Zurich based consultancy, offers a BMM / SBVR integrated technical infrastructure to assist companies with the related definition and transformation processes.

The first problem is to define a suitable syntax for GRC related data, metadata and metadata interchange. OCEG decided to use the industry standard format for business reporting, the eXtensible business reporting language (XBRL (Engel