An OCL Framework for Representing Internal Controls in an REA Framework

By

Dr. Graham Gal University of Massachusetts at Amherst

Dr. Guido Geerts, University of Delaware

Dr. William McCarthy Michigan State University

June 2008

Abstract

The development of large information systems that are capable of meeting the requirements of modern more complex organizations has forced computer science researchers to develop new paradigms in both data structures and software engineering. The ad-hoc techniques that were prevalent in early systems did not scale up to the large systems and thus the disciplines of software engineering and database design sought answers to questions that made the development process more systematic. Today the large ERP systems that integrate the many functional areas of modern organizations require a different approach to the specification of controls. Current ERP systems can include as many as 3000 separate controls that can have multiple configurations. Certainly, some configurations do not make sense, but the sheer number of possible combinations makes an ad hoc approach to their configuration and review increasingly difficult, if not impossible. A continuous review is made even more difficult when the dynamic nature of job and responsibility assignment is considered. Much of the current literature considers controls to ensure that incompatible duties are segregated; however other types of controls are also required for management to maintain a well controlled organization.

Among the responsibilities of management is to specify the way in which the firm will achieve the objectives of the organization. Both the COSO and CobIT frameworks for evaluation of internal controls look at the connection between the objectives and the management control of the organization. This connection was always important, but the passage of the Sarbanes Oxley legislation made the responsibility of management to control the organization more explicit. The events or transactions that occur are the basic activities that further the objectives of the firm and therefore form the basic activities to be controlled. The internal control literature specifically states that these activities must be executed in accordance with management's general or specific authorization. For management to determine that controls are functioning these activities must conform to a structure prescribed by management. The structure of the activities is part of the general description of the ontology of business process and has been formulated within the Resource Events and Agents (REA) model.

The REA ontology describes the events of business organizations as consisting of resources being exchanged between agents as a result of the execution of certain events. The ontology also breaks down the activities into three distinct layers. The initial layer of activities consists of the past and present events in which actual exchanges take place. Examples of events within this layer include sales events in which inventory resources are exchanged between sales agents and customer agents. The summarizations of these events form the traditional financial reports and serve as a basis for evaluating management's ability to achieve the organization's objectives. The next layer in the ontology represents the planning events. Examples of events at this layer include production schedule events where types of raw material resources and types of factory worker agents are combined according to a management plan where types of finished goods will be created at some point in the future. Other examples include the plan for future purchases events of raw materials resources by buyer agents from supplier agents to be used for future production. The reports that summarize these events indicated management's perception of the activities that should be undertaken to achieve the objectives. The final layer of the REA ontology includes the policies prescribed by management as the acceptable way in which the activities of the first two layers can be carried out. Specifications at this level include what types of agents are allowed by management to execute sales events to which customer agents. This

specification falls under the traditional notions of segregation of duties; however there are other types of policies that can and should be expressed.

Management must also express not only what job types are allowed to perform various events and with which resources, but the way in which events must be completed. There are established sequences or workflows that management will specify for the completion of business processes. Thus for a sale event to be accomplished correctly an order must be received from a customer agent and any price or product characteristics must be fully specified. Specifying the acceptable order of events is also a responsibility of management and represents restrictions or constraints on the way objectives can be accomplished.

Traditional views of data models break them down into declarations, procedures, and finally constraints. The policy level of the REA ontology includes the constraints on the way in which an organization's states may change over time. The specification of management's policies in terms of constraints provides a structure to the policy level specifications and therefore a structure on the acceptable future states of the organization. In a functioning organization there are enumerable ways in which a strict adherence to management policy may be violated; a sale may be made to a customer without the necessary credit limit, a person may be hired without all the requirements for a specific position. Summary information about the degree to which the constraints have been violated provides information about the degree to which internal control systems are functioning within the organization – the degree to which management policies are being followed. It is the purpose of this paper to extend the REA ontology to include formal specifications of constraints or management policy.