

SEMANTIC SPECIFICATION OF INTERNAL CONTROLS USING THE RESOURCE-EVENT-AGENT ENTERPRISE ONTOLOGY

Dr. Graham Gal *

Dr. Guido Geerts **

Dr. William E. McCarthy ***¹

Abstract

The development of large information systems that are capable of meeting the requirements of modern 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

¹ * Isenberg School of Management, University of Massachusetts, Amherst, MA 10003 USA gfgal@som.umass.edu

** Alfred Lerner College of Business and Economics, The University of Delaware, Newark, DE 19716 USA
geerts@lerner.udel.edu

*** The Eli Broad College of Business, Michigan State University, East Lansing, MI 48824 USA
mccarthy@bus.msu.edu

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 then 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.

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, a product could be produced using too much of a particular raw material, etc. 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.

Section 1 - Introduction

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 process of development of these objects more more systematic. Most large ERP systems, which integrate the many functional areas of modern organizations, have been developed using one of the software engineering methodologies. However, these systems can require users to adopt the base functionality of the system or to go through extensive customization. There are some approaches that assist in the schema modification (Arinze and Anandarajan 2003), but the current tools do not address the needs of different user groups (Björn and Carvalho 2010). The difficulties with the customization process become even more of an issue with the specification of controls (Qiao, et al. 2007).

Current ERP systems can include a few thousand possible controls which 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 (Colatonio, et al. 2009) . 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 (Committee of Sponsoring Organizations of the Treadway Commission 1994) and CoBIT (IT Governance Institute 2007) frameworks for evaluation of internal controls look at the connection between the objectives and management's 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 and to execute their governance responsibilities 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 then the execution of these activities must occur in a predefined or structured manner as 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, McCarthy 1982) model.

The REA ontology describes the events of business organizations and breaks down these activities into three distinct layers. The initial layer of activities consists of the past and present events in which actual exchanges take place. 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. These events constitute the plan by management to achieve the objectives of the firm. Summarization of these events indicate to management the activities that have been planned or scheduled and 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 parties should execute the firm's activities.

Traditional views of data models break them down into declarations, procedures, and finally constraints. In some systems these constraints are natural; water will be ice at a certain temperature or sound will travel at a certain speed. The predominant type of constraints in a business organization represent restrictions on the way in which the event sequences may take place. These restrictions can be made by external stakeholders; computers with this configuration may not be shipped to customers in country X. They can also be made by the internal stakeholders; shipments must be preceded by customer verification. These restrictions are the policy statements that govern how the actual and planned activities should take place. Thus these policy statements on activities or events form the policy level of the REA ontology and constraint the way in which an organization's states should change over time. The translation of management's policies into formal constraints provides a structure to the policy level specifications and therefore a structure on the acceptable future states of the organization.

These policies are not binding and therefore the constraints derived from the policies may be violated. 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, and so on. Summary information about the degree to which the constraints, or policies, have been violated provides information about the degree to which internal controls systems are functioning within the organization. This paper will look at the translation of policy statements about the activities of the firm into the design of internal control systems. This design science (March and Smith 1995) approach used in this paper will also look at the internal control frameworks proposed by COSO and CoBIT in the design of the constraints within the REA ontology. The frameworks provide a basis for considering pertinent aspects of controls and the REA ontology provides a representation of the relevant objects in a business organization that are components of any control system. This paper will also extend the REA ontology to include the specifications of constraints or management policy.

The remainder of the paper is organized as follows. The next section presents the basic components of the REA ontology. After this will be a more formal discussion of management's role in specifying objectives, policies, and procedures. This will be followed with a specification of the ontological extension to the REA model that includes management policy statements and constraints on the operation of the firm. The final section of the paper discusses the role that these constraints play in the evaluation of a firm's internal controls.

Section 2 – The REA Ontology

Any attempt to formalize the constructs for a domain of discourse has as its central purpose to describe the underlying structure of the target domain. The specification of these structural elements becomes the basis for the ontology of the domain. In this work the particular domain ontology used focuses on the domain of accounting activities (McCarthy 1982). This ontology was extended in ISO 15944 (ISO15944-4 Information Technology - Business Operational View 2007) and includes more activities than those that have strict financial statement or accounting implications. This section will look first at the basic ontology developed by McCarthy (1982) and then the extensions made to it as part of ISO 15944.

The REA Ontology

The REA Enterprise Ontology (REA-EO) describes the accounting domain as a series of value exchanges and is shown in Figure 1 Each event of the firm can be viewed in terms of parties within the firm reaching agreements with external parties to exchange valuable resources. The REA-EO has four object primitives: Resource, Economic Agent, Economic Unit, and Economic Event. Resources can be described as types of goods, services, or rights to goods or services. Cars, tires, buildings, cash, etc are examples of goods that can be acquired or provided, while advertising campaigns, machine maintenance, and consulting advice are examples of services. Each of these types of resources, goods and services, can be viewed as a constellation of attributes. Thus a car has, in addition to its material components, attributes such as the ability to resell it or to loan it to an acquaintance. Owning the car comes with all of the attributes of the car. A right can be viewed as acquiring a good without all of the attributes. So leasing a car comes with most of the attributes one gets if they buy a car except the ability to use it for an unlimited time frame and to resell it. Other examples of rights would include the purchase of music or videos in which the party buying either of these resources does not acquire the right to resell it or make copies of it for other parties.

Agents are either people or organizations with the capacity to enter into the exchanges. Agents are of two types; internal – within the organization and external. Internal agents are types of employees while external agents are types of customers, vendors, creditors, investors, etc. Either of these external agent types could be a person, Joe Jones, or organizations

themselves, Dell Computers Inc. The events are the exchanges of a resource by agents within and external to the organization. These events are paired through reciprocal relationships in which one of the paired event results in a resource being used, decrement event, while the other event in the pair results in the value or quantity of a resource increasing, the increment event².

As shown in Figure 1, the REA-EO also has four relationship primitives. The relationship between resources and events is a stockflow relationship. That is an event results in the stock of a resource to either flow in, increment event, or flow out, decrement event, of the firm. The participation relationship describes the way in which agents come together to execute the events. The duality relationship binds separate increment and decrement economic events (Geerts and McCarthy, Modeling Business Enterprises as Value-Added Process Hierarchies with Resource-Event-Agent Object Templates 1997) into distinct business processes. Finally, the responsibility relationship describes the lines of authority within an organization. Thus, a clerk type of employee works for a manager type, and the manager is responsible for the supervision of clerks under their span of control.

The business processes within a firm are connected to form a value chain; a chain of activities that add value to acquired resources. The original concept of the value chain was presented by Michael Porter (Porter 1985). In this book the activities of the firm were conceptualized as being connected through a series of value adding business processes. In (Geerts and McCarthy 1997) Porter's value chain model was extended to the REA model and related specifically to the transfer of resources between business processes within the firm. In figure 2 the general business processes and the resources transferred between these processes is depicted.

In the Acquisition Business Process the receiving event results in the stock of a resource to flow into from a vendor that deals with a buyer is paired with a cash disbursement event that results in cash flowing out of the firm to the vendor from a cashier. The means of production, resources, are then made available to the Conversion Business Process where activities are performed to transform and add value to the acquired resources. These transformed resources are then made available to the Revenue Business Process where they are exchanged for the cash resource which is then used in the Financing Business Process to repay investors. Within the

² Acquiring advertising services would be an example of an event in which the value of resources increases while the quantity does not.

REA ontology each business process contains their respective pairs of these events connected through the duality relationship. The accounting domain places great importance on the measurement of both the value of resources exchanged in these events as well as the imbalances between the values of the resources exchanged in the events paired in duality relationships. Income statements include various aggregations of events such as sales while the imbalances become central to balance sheet numbers such as accounts receivable for the revenue business process and accounts payable for the acquisition business process.

Within a functioning business enterprise all accounting activity follows McCarthy's REA pattern as (R) resources are exchanged through (E) events by (A) agents. While this pattern corresponds to the activity instances that can or should be captured and represented within financial statements the original REA pattern does not describe all of the activities within a business process. In particular the activities that occur prior to and anticipate the actual exchange of resources; those that are not summarized in accounting statements are not part of the model. These extensions are described in ISO 15944 and represented in Figure 3.

ISO15944 – The Expanded REA Ontology

Prior to the actual exchange of resources business agents go through a number of phases in anticipation of making an exchange. The initial phase is one in which agents consider or plan to make a future exchange. Activities that represent an agents' plan to acquire a resource include the search for information through a request for a catalog from potential collaboration partners. In an ecommerce environment this might take the form of putting search terms about desired resources into a search engine. The result of this initial search is a broad list of potential agents that might be worth collaborating with on a future exchange. The refinement of this list is based on values for certain attributes of the resource; do you have the car in blue? Or the time frame for the possible exchange; do you have the car in stock? This identification phase creates a subset of potential collaborators; those that meet characteristics or fulfill the necessary conditions to move forward and explore the possibility of making an exchange. This agent group is further refined based on the results or fulfillment of negotiation activities.

The negotiation phase includes requirements made by both parties prior to committing to an actual exchange. Rather than simply identifying whether the supplier has a color in stock, during the negotiation phase the requirement that the resource be in a particular color becomes a

necessary condition to commit to the exchange. Rather than identifying whether the resource is in stock there might be a requirement that the resource be delivered in two days. There are two possible results which signal the completion of this phase; either a contract (formal) or commitment (less formal) is established or the parties cannot reach a bargain and further collaborations for the particular resource end.

If the negotiation is successful, the parties agree on the terms of the exchange, and then the actualization phase must fulfill the terms. The initial REA ontology dealt specifically with this phase where actual exchanges of resources occur. In the previous phases the resource exchanges were contemplated and information was exchanged. From an accounting perspective only this actualization phase is represented within the financial statements provided to investors. However, the successful operation of the firm requires information about the phases which provide a basis for the final exchange of resources.

The final phase, post-actualization, occurs if there are subsequent exchanges as a result of issues with the actualization phase. Request for warranty service on the resources exchanged would be an example of such an activity.

Controls and the REA Ontology

Within the various business processes the phases represent the way in which the firm is moving toward financial goals that can be enumerated as values of resources exchanged. The REA model depicted in figure 1 and extended in figure 3 represent the constellation of objects and relationships that serve to organize the data about the firm and its operations. As the firm's business processes operate, data about the activity instances are added to the data structures as described by the REA model. Management is responsible to control the way in which the firm operates. As the data represents the activities of these operations it can provide a means to evaluate the way in which management is controlling the firm and its related operations. In the next section the business processes and their phases will be formally represented using the extended REA Ontology described in this section. This formal representation allows for the control that management exerts over the operations to be represented directly.

Section 3 – Organizational Objectives and Management's Control Responsibilities

This section expands on the REA pattern introduced previously and discusses the concept of internal controls in the context of this pattern. The basic pattern serves as a structure for data that reflects the operations of a business organization. As the firm operates, data is added that provides various levels of detail about the operations of the firm. The structure or pattern by which this data is added serves as a description of the transitions from the business phases or states described earlier. It is the purpose or charge to management to establish internal control systems and it these internal controls which constrain the way transitions unfold as the employees conduct the business of the organization.

Organization Objectives and Management Control

A business organization is run by a management hierarchy that includes an upper level that gives broad direction to the organization and sets objectives for the firm. As one moves down the management hierarchy the responsibility becomes to operationalize these objectives and to determine whether the firm is on track to meet them. Within this hierarchy are types of employees that have a responsibility to perform tasks to achieve these objectives. From a risk management perspective these objectives fall into four areas that have some overlapping characteristics (The Committee of Sponsoring Organizations of the Treadway Commission 2004). The Enterprise Risk Management framework discusses objectives in terms of Strategic, Reporting, Compliance, and Operational objectives and therefore risks, and management must create specific objectives in each of these areas.

In general, reporting objectives deal with reliability of the reports, and reporting risks are those that will create impediments to these objectives. The reporting objectives are primarily imposed by external parties. This is because many of the reporting requirements are the result of mandates by external parties. For instance, a firm must produce financial statements according to rules established by bodies such as the Securities and Exchange Commission (SEC) and the Financial Accounting Standards Board (FASB). Compliance objectives are also generally imposed by external parties that have legal or regulatory power over the firm. These might include taxing authorities, environmental boards, export control boards, etc. To verify either the reporting or compliance objectives have been met requires a review or report on the activities or operations of the firm. Figure 4 shows the relationship of these objectives to the actions of the firm. The reporting requirements correspond to descriptions of certain states of the firm whereas

strategic, compliance and operational objectives correspond to requirements on the way the firm operates and therefore changes from state to state.

Strategic objectives represent the high-level goals of the organization and the process of setting these objectives requires interpretation of the mission of the organization so these high-level objectives are aligned with this mission. Operational objectives specify efficient and effective use of resources. Meeting these objectives requires use of the resources to conform to the strategic objectives and the requirements of the other objectives. For instance, an objective that the company complies with export restrictions on certain products to specific geographic regions constrains the firm's export activities to operate in a certain way. Similarly an objective that reports are reliable essentially means that the reports on the operations match the actual results for those operations.

There are other operational objectives that provide a more strategic direction to the firm. These objectives can come from upper level management and are related to the requirements of specific stakeholders. It is the responsibility of different layers of management to quantify these objectives and to provide control over the activities so these objectives are met. Objectives such as, "... become a major supplier of ...", and "... provide quality customer service ", must be expressed in specific operational objectives. So becoming a major supplier might be expressed as "40% of market share" and "quality customer service", as "deliver products within three days of an order". It is the responsibility of management to formulate policies that will establish a path to achieve these objectives. When the activities or operations of the firm are viewed as causing state changes from a current state to a future state then this future state should have characteristics in which the firm is closer to meeting the objectives than the current state. A central duty of management is to monitor the activities that cause these state transitions and to make an assessment that there is adherence to policies. Internal control constitutes those activities that attempt to make sure the transitions are appropriate, management policies are being followed, and the objectives are being met.

Activities and State Transitions

Figure 5 shows the three possible future states that can result from these state transitions. The first is a state that is completely allowed; a credit sale made by a qualified salesperson to a customer with a good credit rating. This state change would be allowed because the pattern for

the activity is one that is permitted by management. Under all conditions the activities and associated states that result from the process of completing this type of sale are allowed. The state transitions represent adherence to management's policies as they relate to this type of economic event. Financial accounting, and the reports that are central to the discipline, deal specifically with transitions that apply to economic or actualization events, but there are other types of allowed transitions. Allowed states can also apply to transitions that result from tasks in other business phases. For instance, the request for a catalog from a potential vendor is a task within the Planning phase that would result in a state that might also be completely allowed.

A second type of transition is those that are completely not allowed. These could include a state in which a salesperson wants to give a discount that is above the maximum amount. This activity would not be permitted because the activity does not meet the pattern for the "granting discounts" activity type. Other transitions that might be disallowed could include sending merchandise to an agent that has not been appropriately verified. The tasks associated with an "appropriate" verification might be different for specific organizations. However, the state "sending of merchandise to an external agent" will be disallowed unless the state "external agent has been verified" has been reached. This is an extremely important point: certain future states will be contingent upon completion of other states and the tasks required to get to that state may differ between organizations. However, the progression from state to state will not be different – merchandise should not be sent on credit to an unverified external agent. It is whether the preconditions are met that determines that a future state is allowed. In a subsequent section of this paper these states will be more completely defined.

In the first two states the pattern of either the allowed or disallowed states are quite straightforward however the final pattern is harder to specify. The final type of transition concerns those states for which the appropriateness is unsure, and includes the more interesting cases or patterns for the evaluation of internal controls. Outside or other factors must be considered when determining whether these transitions represent control problems. There is a critical distinction between information that should be considered when evaluating controls over state transitions and the evaluation process itself. Examples of transitions for which the appropriateness is unsure might include purchases whose amount are less than \$500 when the firm has a policy that all purchases over \$500 must be approved by a senior manager. The existence of a few purchases just under this threshold is probably not an indication of a problem;

however at some point there would be an assumption that employees are creating purchases in such a way so as to avoid that approval and an important control for an activity is being circumvented. In this example the evaluation of internal controls would look not just at one instance of the set of purchase activities, but at the pattern for a group of instances for that type of activity.

Activity Type Hierarchy

In each of these three cases the central point is that activities are creating state transitions and it is these transitions that must be controlled. In Figure 6a the Activity Type hierarchy is depicted and shows the general organization for the activities within the firm. The first layers of this activity hierarchy show the business processes or transaction cycles. The activities constitute the transitions necessary to complete the requirements or operational goals of business processes such as the Acquisition business process, the Revenue business process, or the Hiring of Employees business process (a subset of the general Acquisition business process). In each business process the activities correspond to the steps that need completion for an accepted completion state of the process. These steps are organized around phases that specify the temporal order of activities required within the each business process (ISO15944-4 Information Technology - Business Operational View 2007). These phases include:

1. Planning – activities to decide what action to take for acquiring or selling a resource
2. Identification - Activities to exchange information among potential parties
3. Negotiation - Activities to achieve an explicit, mutually understood, and agreed upon goal of a business collaboration
4. Actualization – Activities necessary to execute the results of the negotiation
5. Post-Actualization – Activities that occur after the agreed upon resource has been delivered

These activities may have temporal dependencies; certain state transitions could rely on conditions from another state. For instance, within the Revenue Business process the activities associated with determining the credit worthiness of a customer should be completed prior those activities associated with shipping merchandise are initiated. The phases are consistent across the Business Processes, but can be further decomposed depending on managements' imposed structure for the activities.

The management of one firm could consider Financing as a single process while another could recognize distinct processes for long term bonds and financing done by selling commercial paper. The types of activities for each of these financing sub-processes would still complete the same phases, but may require different tasks. For the financing of long term bonds the tasks of the planning process may be more entailed, but the planning activity for selling commercial paper would still be done. This same decomposition can be done across all of the business processes and represents the structure or span of control allowed by management. Thus permission may be granted to control the Acquisition Business Process or only to the Raw Material Acquisition Business Process, or even at a level further down the Activity Type hierarchy for Large Sales in the Revenue Business Process that pertain to overseas shipments. This separation of activities within the organization is central to the notion of segregation of duties (Rittenberg and Schwieger 2001). To control the state of completing a particular business process the authorization of the process should be separated from performance and review of the activities within the process. As information systems become more automated the recording of the information about an activity is done as part of the activity itself, but the review of the process still should be segregated from the performance. One role of management is to delegate tasks in such a way so that no single employee can perform an activity and also review it. Thus permissions to perform activities are divided within the employee hierarchy with the segregation objective as a central factor.

The phases of each business process include tasks or activities that management would require to complete or further the phase. The Planning phase would include activities to either send out or obtain information about a resource while Actualization Phase can be decomposed into activities required by management to complete increment and decrement events. This structure allows for specification of permissions at different levels in each hierarchy. Permission can be granted to perform activities at the Revenue Process Level or only for Negotiation activities associated with Acquisitions of Advertising Services. The activities can be specified at increasing levels of granularity and would be decomposed to the level of detail to which management wants to exercise control. If there is a desire to control who is allowed to call a vendor to ask about prices then the Activity Type hierarchy must be specified down to that level of detail. There are also activities that might not be considered to be directly related to the goals of a specific business process, but are necessary to establish control within the business process.

When a manager establishes control over a business process there are some policies for activities not directly contained within the process but are considered more general activities. Setting characteristics and qualifications for employee types is such an activity. Establishing qualifications for employee types is not central to the verification of credit worthiness activity, but the proper control over this process is enhanced if a qualified person is performing the activity. This precondition that the state in which formal job descriptions precede actual hiring activities can also be viewed in terms of states that might be allowed, and require monitoring. From a control evaluation perspective if one position does not have a formal description then this might not be an issue. However, if the position is critical to a critical process then this might be a condition that would disallow or cause control issues for subsequent states in that process. These formal job descriptions include the different types of job functions.

Employee Type Hierarchy

The formal descriptions of Employee Types allow for employee instances to be assigned to a type and the activities they are allowed to perform as a member of that type. The purpose of established lines of authority in the firm allows for task assignment to employee types. The hierarchy depicted in Figure 6b shows the structure of Employee Types which becomes central to the descriptions of positions and the establishing of formal skills, knowledge levels, or other requirements for each of the job functions within the firm. Figure 6c shows the superior – subordinate structure and is central to the assignment of responsibility by management, the span of control for particular Employee Types, and the appropriate segregation of duties. While these two sets of dimensions with the Employee Types are related they provide different types of control.

The Employee Type superior - subordinate descriptions ensure that authority is delineated within the firm while the specification of knowledge and skill levels by Employee Type ensures a level of competence to perform the specified activities. The activities to establish job descriptions and skill requirements do result in new states (the state where the job has been described) and it could be argued that the state does not directly further the objectives of the business process, but instead sets a tone for the organization's other activities. The COSO (The Committee of Sponsoring Organizations of the Treadway Commission 2004) framework for the evaluation of internal controls places these activities under the general category of the control

environment. The control environment establishes an underlying structure to ensure the business processes function as designed. For instance, establishing job descriptions and skill levels does not necessarily ensure that a specific activity within a business process will be done correctly, it does ensure that an activity, or task, will be assigned to a type of an employee with a level of skill as required by management.

The hierarchical structure of the firm links different employee types that either have the responsibility to perform a particular set or types of activities, or the authority to delegate the activities to subordinate employee types³. Each type of activity is linked to a specific business object within the firm. These objects correspond to the constructs of the REA model. This basic structure, shown in Figure 7 forms the basis of permissions within the firm and management's policies with respect to how the firm should accomplish the various tasks associated with achieving the overall objectives.

Permission Structure

Within each business process the activities are delegated to or are the responsibility of a particular type of employee. For instance, the Vice President of the revenue process has the authority to perform all the activities within the business process, but also to delegate the activities to subordinates. The Vice President can play either the role of performing the activity or the role of delegator (shown in Figure 6d). Further down the hierarchy the authority to delegate is removed while the responsibility to perform remains: the credit manager Employee Type has the responsibility to perform a credit check, but cannot delegate tasks associated with this activity to a subordinate Employee Type.

Additionally the Activity Types are restricted to a particular business object; the credit manager (employee type) can perform (job function) the credit verification credit (activity type) for a customer (business object). In the raw material acquisition business process the vice president of purchasing (employee type) can delegate (job function) the delivery terms (activity

³ The CoBIT (IT Governance Institute 2007) framework presents a RACI chart which breaks down processes within an enterprise's information technology area into types of employees that are responsible, accountable, informed, and/or consulted. So a type of employee can be responsible to perform a process while someone up the hierarchy can be held accountable for the performance of a process.

type) for raw materials (business object). This constellation of job function, activity, and object form the basic structure of a management policy concerning the delegation of responsibility and is a central component of firm's internal controls. This same permission structure (figure 6) can be applied to the tasks that further the control environment within each business process; the vice president of marketing (employee type) can perform (job function) the process of establishing the level of training (activity) and responsibility for tasks (activity) for regional sales manager (business object – agent).

This structure also allows for the design of the business processes that encompass these activities so as to achieve the enumerated objectives of the firm. The permissions establish control over the state changes within the business processes and it is these state changes that further the business in meeting the objectives. Permissions can be granted at any level of the Employee Types, Business Objects, or Activity Types.

These permissions to perform various activities can also be connected to other permissions. There are four types of connections that are possible between permissions; temporal, inclusive, exclusive, and no restrictions. Temporal connection between permissions indicates that there are required state changes prior to permission to perform activities related to subsequent state changes – all the conditions must be negotiated before a purchase is made. A second type of connection is inclusive – if a person is hired they must be assigned to an employee type. An opposite connection is the exclusive relationship between permissions – if the negotiation activities have failed state then actualization cannot occur. Finally there are permissions for which there are not any conditions – a salesperson can always send a catalog to a soon-to-be customer. The connection between permissions is shown in figure 8. The next section of this paper demonstrates how this framework for specification of controls in terms of permissions can be represented using constraints specified in the object constraint language (OCL, Warmer and Kleppe 1999).

Section 4 – Management Policy and Constraint Specification

In the previous sections of this paper the pattern for the underlying structure of the types of activities and the types of employees that operate a corporation were specified. The ability of employee types to delegate the responsibility to perform various types of activities and to delineate specific organizational areas is central to the management function of setting policy,

controlling the operations of the firm, and separating incompatible functions. Controlling the operations is an important part of the process of ensuring the firm progresses towards states in which objectives of the firm are met. Exercising control over the operations of the firm also supports the meeting of strategic and compliance objectives as well. This control function serves to constrain the firm to operate according to some pre-identified patterns specified by management.

At the highest level the activities are organized around different business processes within the corporate value chain. These business processes can be further specialized around more specific subtypes of the general business processes. Within each business process the activities are further organized around phases of the business process. These phases are defined in the extended REA model, ISO15944, and reflect the stages by which the business process progresses toward its goals and supports the meeting of the overall corporate goals and objectives. Each business process subtype includes these phases although the specific tasks for the phase may differ. For fixed asset acquisition the planning phase might entail a review of only a few industrial suppliers that make the specific machine while the planning phase for the activity type, “raw material acquisition,” might entail a much broader review to see what vendors carry a type of material. To control the performance of the activities that result in state changes within the business processes management grants various types of permissions.

The permission to delegate activities within the business processes is a major aspect of managing the firm. This management of activities by delegation to appropriate employee types is central to controlling the state changes that result from the activity and separating incompatible functions. At the lower levels of the organization are those employee types that cannot delegate further and only have the authority to perform activities. The actual performance of these activities result in state changes within the business processes and move the firm closer to meeting the stated objectives. The state changes that result in the granting of permissions to delegate and to perform activities is part of the process of setting internal controls and establishing policies or patterns for the permissions to perform these activities.

The Setting of Permissions

The setting of permissions within the firm establishes both responsibility and authority for activities and is a central activity for management in establishing internal controls. If the

permissions were specified at the instance level this control activity would soon overwhelm management. One important aspect of any administration of permissions is the ability to scale to large settings such as ERP systems (Li and Mao, Administration in Role-Based Access Control 2007). Rather than specify permission at the instance level, the patterns for the objects in Figures 6(a – d) allow for the specification of permissions as constraints to be applied at the type level and enforced on instances of these types. The delegation of permissions allows for management to exercise authority over the types of employees and the types of activities within their organizational span of control, thus reducing the complexity of the processes of establishing internal controls by establishing predefined areas of the organization. The pattern for these permissions is specified in terms of business object types (those objects for which the activity is assigned), job function (delegate or perform), employee types, and activity types (see figure 7). The permissions structure must also take into account the established superior- subordinate relationships.

This span of control pattern also ensures that the hierarchical structure can be explicitly included in the permissions. These established permissions then represent constraints on the way in which activities are assigned, delegated, and performed. The permission for an activity entails specifying types to fill in the slots for the general permission and would be represented in the Object Constraint Language - OCL (Warmer and Kleppe 1999) as follows:

```

Transaction:: Permission (b : BusinessObject, j :JobFunction, e : EmployeeType s : EmployeeType, a :
ActivityType)
pre : Superior(s,e) and Select (EmployeeType = s) -> forAll (
    DelegateActivities -> includes (b, a)
    and PerformActivities -> includes(b, a)
)
post : if j=#delegate then Role -> select (employeeType = e) -> forAll(
    DelegateActivities = DelegateActivities@pre -> including(b, a) and
    PerformActivities = PerformActivities@pre -> including(b, a)
    Else
    If j=#perform then Role -> select(employeeType = e)(
    (PerformActivities=PerformActivities@pre -> including(b,a)
    )
    Endif
    Endif

```

This OCL statement should be interpreted as: if the preconditions (pre:) that employee type (s) is Superior to employee type (e) and that the activity type is included in both the superior's

delegation and perform activities⁴ then perform the post steps. If the precondition is met then the post condition (post:) results in addition to the Role for the selected employee type this new permission. If the permission is to delegate then the activity type (a) on the object (b) is added to the list of both the activities the employee type can delegate and can perform. If the permission is only to perform a type of activity then this activity is only added to the list of Perform Activities for the Role of the specified employee type (e). This means that a Role for a particular employee type consists of the activity types that can be delegated and those that can be performed along with the objects on which the activity types can be performed. For example a Vice President's role includes assigning negotiation activities and performing division review.

The policy statement, "The Chief Operating Officer (COO) delegates permission to the VP of Sales to delegate all activities associated within the Revenue Business Process," would be represented with the following permission:

Transaction::Permissions

P.Delegate.Revenue{b.Resource,jt.Delegate,e.VicePresident.sales,s.COO,at.Revenue}

This delegation would only be allowed if it was made by an employee instance filling the employee type of the "Chief Operation Officer", the COO type is a superior of the Sales Vice President type, and COO type has the authority to delegate this activity in their collection of delegation activities within their Role. After this permission has been made an employee instance that has been assigned to the employee type "Vice President of Sales" can delegate further down the employee type hierarchy to those employee types that are within their span of control. A Sales Vice President instance can now grant further permissions such as to a sales manager type the ability to perform the negotiation activities for inventory items:

P.Perform.Revenue.Negotiation{b.Resource.Inventory,jt.Perform,e.SalesManager,s.VicePresident.sales,at.Revenue.Negotiate}

Or to delegate to someone subordinate to them:

P.Delegate.Revenue.Negotiation{b.Resource.Inventory,jt.Delegate,e.SalesManager,s.VicePresident.sales,at.Revenue.Negotiate}

⁴ The permission of the employee type to delegate must include the permission to perform that activity as well; a person that can delegate must also be permitted to perform.

This permission would allow the sales manager to perform all the negotiation activities, but also to delegate them further down the span of control hierarchy. This is allowed because of the permission granted to the Vice President. Now the sales manager can delegate activities as follows:

```
P.Delegate.Revenue.Negotiation.setprices{b.Resource.Inventory, jt.Perform, e.StoreManager, s.SalesManager, at.Revenue.Negotiate.setprices }
```

This permission would be allowed because the type “store managers” are in a subordinate relationship with sales managers types, the type sales managers’ role includes these negotiation activities in their delegation activities, and setting prices is an activity type that is contained within the negotiation phase. The semantics of the administration of these permissions matches the responsibility relationship proposed in the original REA model and the common management structure found in most organizations, and therefore the “psychological acceptability” design requirement suggested by Li and Mao (Li and Mao, Administration in Role-Based Access Control 2007).

Establishing the Superior-Subordinate Structure

The superior-subordinate structure depicted in figure 6c is central to the process of establishing lines of authority and the permission to delegate and to perform activities. The segregation of incompatible functions is dependent on assigning activities in such a way so that no employee type can both perform an activity and also review the activity to verify that it has been done correctly (Rittenberg and Schwieger 2001). The fundamental authorization and therefore review of activities rests with the Board of Directors and the Chief Executive Officer (CEO). The formation of the permission structure is dependent on the Board and CEO establishing the Employee Type hierarchy and then connecting the higher level Activity Types to this structure. When an activity is delegated the review rests with the person doing the delegation. The general permission structure can be specified within the structure depicted in the previous section and the establishment of the superior-subordinate hierarchy would be set as follows:

```
EmployeeHierarchy::EstablishEmployeeHierarchy(superior:EmployeeType,  
subordinate:EmployeeType)
```

Post : Assignedto (superior, ?et) = Assignedto(superior, ?et)@pre - > including (?et = subordinate)

This statement would be interpreted as the post condition for the EstablishEmployeeHierarchy event is that the subordinate EmployeeType is now Assignedto the superior EmployeeType. We could also add another post condition that establishes the test of the Superior function used in the permission.

Post: Superior (superior, subordinate) - > true

The entire Employee Type hierarchy can be reviewed by testing for superior – subordinate assignment and the segregation of duties can be enforced along the lines of this established structure. This allows for assignment of activities only to those Employee Types that report to or are assigned to a particular Employee Type. The original permission had two preconditions but there are others that can be accommodated in permission structure. One such precondition concerns the existence of certain state preconditions such as the customer verified state must exist prior to the activity of shipping merchandise.

Establishing Relationships between Permissions

Temporal State Conditions

In section 3 three types of additional conditions that could be enforced on permissions were identified. The first concerned the temporal or preconditions on permissions. This type of permission is based on the completion of states and therefore the states on which the conditions are based must be defined. The phases of the extended REA model provide a connection to states and the activities within the phases define the progression or steps required for the phase. The general example concerns the completion of the negotiation phase prior to the actualization phase. This can be viewed as completing the state of negotiating or setting the terms of the contract prior to executing the steps or activities to execute the contract. In the revenue business process this would mean formalizing an agreement with a customer prior to shipment of merchandise. The steps for completion of the negotiation state, and therefore the agreement, could include activities related to setting prices, delivery dates, payment terms, etc. These activities could take place in any order, although there might be some reasons to put conditions on the order for these activities as well. However, at some point the activities required by the organization to proceed to the next phase will be completed and the negotiation state will be in

state complete. This precondition that negotiation be complete prior to actualization can be added to the general permission for all business processes:

P.Actualization(bot.event, jt.perform, et.employeetype, st.employeetype, at.actualize)
Pre : Negotiation.state = #complete

If the permission is for a particular business process then permission can be refined. As an example within the Acquisition business process the person receiving merchandise in the warehouse might have permission to receive merchandise, but within the Revenue business process nothing can occur in the Actualization phase until the negotiation phase is complete:

P.Revenue.Actualization (bot.Revenue.Events, jt.Perform, et.employeetype, st.employeetype, at.Revenue.Actualize)

Pre: Revenue.Negotiation.state = #complete

Or, it can be specified at the specific activity type level so that the warehouse clerk can accept the merchandise, but cannot transfer the merchandise into regular stock:

P.Acquisition.Merchandise.Actualization(bot.Acquisition.Events, jt.Perform, st.WarehouseManager, et.WarehouseClerk, at.Acquisition.Actualize.TransferToStock)

Pre: Acquisition.Merchandise.Negotiation.state = #complete

Within the Acquisition business process this could apply to other types of Acquisitions such as the receipt of fixed assets. The important part of specifying the temporal order of permissions is the definition of the states and the activities that bring upon the states. In the ISO15944 report a number of different states are enumerated (p. 39). The important issue for the setting of the condition on permissions and therefore the activity instances allowed by the permissions is for management to specify the activity type that brings about the particular state. Once specified, these states can be tested for completion (Gal, et al. 2010). Another type of connection between permissions is also related to states and includes those permissions that are inclusive, i.e. those permissions that are connected to each other and those that are exclusive or not connected.

Inclusive and Exclusive Permissions

The general permission structure must consider permission types and activities that either must be included or excluded from each other. In the OCL for the general permission the

delegation permission includes the perform permission. This means that an employee type that has permission to delegate to a subordinate also retains the permission to perform the activity as well. From a practical standpoint, if an organization did not have any instances of a particular employee type then an employee type higher up the hierarchy would still be able to perform the activity normally the responsibility of a subordinate. This can also be viewed from the more general perspective of roles within the organization. Certain employee types such as Vice Presidents or Managers must have permissions to run their part of the organization and therefore roles for employee types must include all the permissions to complete the business process assigned to them. The need to include permissions to groups of activity types is similar to the Named Protection Domains (NAD) introduced by (Baldwin 1990).

These NADs included privileges on objects assigned to different users. The objects in Baldwin are similar to the activity types and business object types in the proposed permission structure. The activities in the NAD model are more granular and correspond to the database transactions of Select, Update, Add, and Delete. The activities in the hierarchy portrayed in figure 6a support this concept at various levels and include higher level tasks, such as “set prices” which would include a number of the lower level transactions. The hierarchical structure of the activities allows for a high level of inclusion around different roles within employee types.

Permission to perform all of the activities associated with the Negotiation phase allows for inclusion of all of the tasks or steps that a firm specifies as relevant for this phase. The delegation process allows for including activities at the level of granularity as required by management. The Vice Presidents can be delegated all the activities associated with the Revenue Process, while the store managers can be delegate a subset based on management’s review of the processes required to complete the manager’s responsibilities. This delegation of the permissions throughout the employee type hierarchy meets the scalability condition for administration of role based access control (Li and Mao, 2007). In contrast to the inclusive permissions are those that must be separated or not included in the same role.

The Role concept has been used to enforce computer security (Li, Tripunitara and Bisri, 2007) as an approach to separate duties, but also to provide necessary permissions to complete tasks. In the security context the separation allows for cooperation of individuals while maintaining inability to perform the entire set of tasks. The static separation of duties (SSoD) are enforced using statically mutually exclusive roles (SMER). In this context the n steps

required to complete a sensitive task are split among k individuals ($k \leq n$) that must cooperate. The static assignment of tasks is based on instances and could result in violation of the separation of duties if an instance is reassigned prior to the completion of the entire task instance. To overcome this eventuality dynamic separation of duties DSoD (Nash and Poland 1990) was formally defined in terms of histories of the task instances with employee instances. This dynamic separation of duties can also be enforced at the type level.

Separation of duties requires incompatible functions to be excluded from different levels of the employee type hierarchy. The REA model allows for certain types of separation of duties to be expressed directly as opposed to on an ad hoc basis. The duality relationship connects events that from a separation of duties perspective should be carried out by distinct employee types within certain business processes. In each business process the events that are paired in the duality relationship are increment and decrement events. Within the Revenue business process this duality relationship connects the Sale (decrement resources) with the Cash Receipt (increment resources – cash). To enforce separation of duties the same employee type should be not be able connected to both of these events. In the best case these employee types should come from different parts of the hierarchy – Treasurer for activities related to the resource cash and VP Sales for activities related to the resource goods for sale. This can be expressed with the following constraint:

$$\text{IsEmpty}(p(\text{bot.revenue.sale}, \text{pt.x}, \text{st.s}, \text{et.e}, \text{at.a}) \cap p(\text{bot.revenue.cashreceipt}, \text{pt.x}, \text{st.s}, \text{et.e}, \text{at.a}))$$

Or for a more general case:

$$\text{IsEmpty}(p(\text{bot.bp.event.increment}, \text{pt.x}, \text{st.s}, \text{et.e}, \text{at.a}) \cap p(\text{bot.bp.event.decrement}, \text{pt.x}, \text{st.s}, \text{et.e}, \text{at.a}))$$

As was the case with the inclusive permissions, the specification of activities types and employee types in the hierarchical structure allows management to create roles and to separate incompatible duties perspective at the level of granularity desired. The Roles consist of activities that can be performed and those that can be delegated. This model allows for a relationship between employee types at different levels of the hierarchy and the roles that can be performed. This structure allows for a dynamic specification of duties. When an employee

instance is reassigned to a different employee type it would be essential to remove them from one employee type as part of the transfer:

Permission to perform the transfer activity

P.Actualize.Transfer(bot.event.assign,pt.perform, st.VPHumanResources,
e.ManagerHumanResources, at.actualize.transfer)

Transfer performed

EmployeeType :: Transfer(employee.e, EmployeeType.et)
Post : Remove (e, Roles.e) and Assign (e, et.Roles)

Again this action could result in the employee instance being able to perform activities that should be separated, but the review of the permission structure would be a factor in the decision of whether there is a control problem within the firm. This approach can handle the situation in which someone has been reassigned, however in a functioning business organization there are other issues that should be considered.

While there is a possibility that an employee instance may be reassigned to positions that would lead to violation of separation of duties at the activity instance level this must be considered in the context of the business processes of the firm. When a review⁵ of the violations at the instance level is performed other information becomes relevant. The definition of Employee Types includes the specification of the characteristics for that type; minimum level of education, age, citizenship requirements, skill set, etc. When an instance is assigned to a employee type the degree of that match is also considered. Even if there weren't any violations of SoD at the instance level, if there were mismatches in the assignment of instances to employee types there could still be an internal control issue. If the permissions to perform and delegate human resource activities within a firm are assigned to appropriate employee types in the hierarchy then the evaluation of DSoD would be different than the evaluation of a firm where the assignments are not appropriate. Earlier in this paper the notion of evaluation of controls as being separated from the specification of data to be considered was raised. This point is relevant with the separation of duties evaluation as well. Another issue that is related to the separation of

⁵ In the next section the concept of internal control evaluation will be considered. It is important to make a distinction between evidence and the evaluations made using that evidence.

duties is the appropriate way to add tasks in such a way that they do not conflict with previous assignments.

Adding Activities to Business Process Phases

A functioning firm should continually evaluate the activities for each business process. This review can be performed by either internal or independent auditors on a regular basis. Under Section 404 of the Sarbanes Oxley legislation (United States General Laws 2002) a review is required as part of the yearly audit and must include a statement about any material weakness in the internal control system. From a control perspective this evaluation can determine a weakness because certain activities should be done by a different employee type because it requires a different level of skill or expertise, should be done in a different order, or should include different steps.

The first condition can be handled within the permission structure by removing a perform permission at a particular level of the hierarchy if it was determined that the activity should be performed at a higher skill or knowledge level, or even assigning the perform permission at a lower level of the hierarchy. The second condition can be handled by defining states at a more granular level and then adding this state as a precondition to the permission for dependent activities. The last condition requires some additional considerations.

In many cases the activities included in the permission structure do not include all of the steps that actually take place in the completion of a phase or even NAD. In a retail example inventory must be moved from the back room to the shelves before it can be sold or the manager must check different pieces of information prior to placing an order. At one stage of development of the activity hierarchy the individual steps may not be explicitly identified and permissions assigned one level above – “receive inventory” or “place order”. If management takes a decision that the implicit steps should be represented explicitly then the activity type hierarchy and the permission structure can accommodate the addition of these detailed tasks directly.

Given the current state of technology it is clear that any step can be explicitly included; even the sending of email steps; 1) click on contact list, 2) click on central warehouse manager, 3) enter “more inventory” in subject, 4) could be included and even monitored. The decision to add activities depends on management’s desire to plan, control, and evaluate the added activities

or steps. Specifically management must decide if they want to plan the steps – determine the appropriate method and time, control – include information about the actual method and time, and then evaluate – look for variances. If it were determined that an additional activity type to the hierarchy this can be done as follows:

ActivityType::AddActivity(AT.Revenue.Actualize.Sales. ReCalculatePrice)

The way permissions are specified, adding new activity types would have only local effects depending on the level the original permissions were made, i.e., it would not impact steps at a higher level activity type. If permissions were specified at the actualization of sales level as opposed to the various steps to complete the sale, then this new activity or step would be incorporated into the original permission structure and the same perform and delegate permission would apply. This depends again on the granularity of the permissions created within the system.

This section has examined a representation of permission structures within the type hierarchies specified in section three of this paper. The use of hierarchies allows the control over the activities of the organization to be carried out at the level or span of control desired by management. This allows management to scale this approach to granting of permissions to the level of control desired; delegation can remain at the very highest levels of management and only perform permissions granted or the delegation permissions can be granted further down the employee hierarchy. A second design consideration concerns the psychological acceptability of the mechanism (Li and Mao, Administration in Role-Based Access Control 2007). There are two issues raised in this area. The first is the interface mechanism, which is beyond the scope of this paper, but the other is the mental image of the goals should match the mechanism.

In discussing the semantics of any particular representation (Obrst 2003) stresses the degree of interoperability of any particular representation. The REA ontology is represented at the frame level. The formulation of permissions in OCL allows for a level of semantics that provides a higher level of interoperability.

The next section of this paper will look at the issue of how the REA ontology and this approach to developing constraints fits into the evaluation of internal controls.

Section 5 – Evaluation of Internal Controls

In a functioning business organization internal controls restrict or constrain the activities of the firm and thus the future allowable states. To establish a system of controls management must consider the ideal organizational span of control and the types of activities that should be assigned to the various business units. The permission framework developed in the previous section provides a link between the business processes and objects described in the REA ontology and the activities required to realize the objectives of the firm. The evaluation of internal control systems must take into account two types of information: the permission structure and the activity instances that create the actual future states. Each of these pieces of information become part of the evaluation required as part of an audit and more recently Section 404 of the Sarbanes-Oxley act (United States General Laws 2002).

Evaluation of the Permission Structure

The permission structure implemented in a specific organization represents managements' perception of the appropriate way each business process should be carried out. It is possible that management has structured these permissions incorrectly. One reason concerns the complexity of the implementation process required by various ERP systems. The number of possible combinations and the methods used in these systems can make assigning permission by management a daunting task. This issue of the psychological acceptability (Li and Mao 2007) is an important requirement for developing permissions and roles within the organization. The development of permissions using the concepts central to management including types of activities and types of employees incorporates the semantics of a very natural business ontology. However, even allowing management to specify permissions in terms of the REA ontology can still lead to incorrect specification of permissions.

When evaluating specific business processes or business sub-processes there are some generally accepted "correct" progression of steps. For the activity type, "credit sale" which is part of the Negotiation phase of the Revenue Business Process there are some steps that in a "well controlled" firm would be followed. The trigger for this sub-process would be the receipt of an order from a verified and credit worthy customer. Therefore the permissions for most subsequent steps in this "credit sale" process must have the state "approved order" as a precondition and this state would include the activity types required to reach that state. If management does not create this precondition for permissions on the later tasks, then there is a

basis for citing this sub-process as having a material weakness⁶. This does not require a review of the credit sale instances to make this determination only the review of the permission structure for the activity type is needed. The subsequent steps include those in the Actualization Phase although not all of them might need this precondition.

There is a distinction in the evaluation of control weaknesses between those that would result in possible incorrect financial statement values and those that simply are not best practices. If the activity type “pull inventory from warehouse” does not have the “valid order” precondition there is not a material control weakness only an inefficiency. If the order never reaches the “approved” state, then the items would need to be restocked; this is inefficient, but does not change a financial statement amount so from an accounting perspective this would not be a material weakness.

The permission structure essentially creates an accepted flow of tasks to accomplish steps in the particular business processes. The evaluation of this accepted sequence implies that management has established an appropriate policy with regards to the running of the organization. While this is a critical first phase in the evaluation the degree to which the instances of the activity types match this flow is central to the review of the internal control system.

Evaluation of Activity Instances

The basis for establishing patterns for the flow of steps in the different business processes is to provide a path for the operations so as to achieve the objectives set by management. In a functioning business organization adherence to these accepted patterns is not always possible. So even if the permission structure is perfect and the prescribed steps to complete the necessary business processes include a perfect progression of activity types there still could be internal control issues. Therefore the evaluation of internal controls includes the review of instances of the activity types.

In the COSO framework (Committee of Sponsoring Organizations of the Treadway Commission 1994) there are basically four components in the evaluation of internal controls. These include the control environment, the risk assessment performed by management, the

⁶ In this context material should be interpreted as serious. In the evaluation of values on financial statements the term material should be interpreted as misleading.

established control activities, and finally the monitoring. The permission structure proposed in this paper fits into this model in a number of different areas.

The Control Environment

The control environment concerns the tone of management with respect (Rittenberg and Schwieger 2001) to controls. This area includes such characteristics of the firm as management's philosophy and operation style, organization structure, board of directors and audit committee, human resources policies and practices, integrity and ethical values, and commitment to competence. There is some guidance Auditing Statement 2 (Public Company Accounting Oversight Board 2007) in terms of the evaluation, but the evaluation is somewhat subjective. However, the permission structure presented does provide some of the information required.

A well-controlled company clearly defines the span of control and the superior-subordinate structure makes this span of control explicit. (Rittenberg and Schwieger 2001). While it is not specifically determined the weight that this factor should play in the evaluation it is clear that the permission structure can delineate the level at which activities are delegated and which types have the responsibility to perform the activity type. The evaluation of instances of activities will be reviewed to see whether this policy is actually followed. A second area within the control environment that can be explicitly represented in the proposed permission structure concerns the human resources policies and practices.

Earlier in the paper the notion of characteristics of employee types was presented. The point was made the while assigning an activity to a well qualified person does not ensure that the instances for that activity will match the accepted pattern perfectly there is a better chance of that happening. For this reason the evaluation of the control environment looks at the degree to which characteristics of the ideal employee type are specified, and the degree to which the policy of hiring qualified employees is adhered to. The specification of employee types and their characteristics is central to the evaluation of the organization's notion of what it means to be qualified. If the employee type "network engineer" does not require any background in networking standards then an auditor could question whether the characteristics of this employee type are designed correctly irrespective of any individuals that actually fill the position. On the other hand there will be situations in which the firm may not be able to fill a position with a

person that is ultimately qualified according to the characteristics for the employee type. The evaluation of whether this would cause an internal control weakness depends on a subjective determination of the frequency that this happens, the importance of the position for specific processes, the determination of which processes are critical, etc. The policies with regard to human resources policies and practices along with the commitment to competence can be evaluated based on the employee type hierarchy component of the permissions. However, the actual evaluation again depends on the subjective determination of the degree to which these control environment factors impact the control over the business processes.

Controlling the Activities

The superior-subordinate relationship along with the specification of employee types within this hierarchy are directly related to components of the control environment and therefore are important in the evaluation of internal controls. These factors impact the evaluation of the internal controls in the business processes themselves. The control activities component is explicitly related to the permission structure presented.

Control activities incorporate the policies and procedures management has established to ensure that errors and irregularities are prevented or detected (Public Company Accounting Oversight Board 2007). From the implementation of the permissions this can be viewed in terms of how exceptions are to be dealt with. At one firm no one could be hired that does not explicitly meet the standards, controls prevent an irregularity, or at another a person without all the qualification is hired and this irregularity is detected⁷. These policies are directly related to the control exercised by management to move the firm toward the organization's objectives and direct the state changes. If management directives are carried out correctly, then their policies are being adhered to and the company is in control. Permissions are the direct representation of these policies. The determination of the states and the permissions to carry out the activities that achieve these states represent these directives and the degree to which the activity instances match the established permission structure determines whether management directives are being followed.

⁷ This view corresponds to the notion of throwing exceptions and writing procedures to catch the thrown exception. The approach to "catching" exceptions is part of the management philosophy.

In a functioning firm the policies will not necessarily be adhered to for all instances. There may be some situations in which merchandise is shipped to a customer before all the steps in the order approval have been completed. Because of the way in which employees are transferred between positions within the firm there could be instances in which dynamic separation of duties at the instance level is violated. Realistically, firms make choices between strict adherence to policies and expediency to accomplish overall objectives. The information and communication and monitoring components of the COSO framework (Committee of Sponsoring Organizations of the Treadway Commission 1994) discuss the internal control monitoring framework along with the capture and review of these exceptions.

The information and communication refers to the collection of all valid transactions. Valid transactions include information about the steps that occur during the operation of the firm. The detail concerns the degree to which management wants to plan, control, and evaluate. Management might want to know that a credit application has been approved, or all the steps taken to make the approval. The activity type hierarchy can incorporate any degree of granularity required by management, and create permissions at this level as well. The instances for each of these steps can be compared to the permission structure and exceptions noted; at the level of granularity that matches the activity type granularity and therefore the degree to which management wants to control the organization. The exceptions to this permission structure correspond to violations of management policy and therefore control exceptions that must be monitored.

Figure 9 shows the relationship between the frameworks for permissions and the REA framework as representations of the established policies and the collection of exceptions. The permission structure provides a framework for representing management policy with respect to performing the activities in a specified pattern as part of the operations of the firm. When exceptions occur the question that faces the auditor is whether the identified policy exceptions represent a serious or material weakness in the operations of the firm. The collection of these exceptions corresponds to the number of exceptions that have occurred over a particular time period. At different points in time these exceptions must be monitored or reviewed; there is a distinction between the method used to identify exceptions, the permissions and the REA framework, the collection of these exceptions, and finally the monitoring. The timing of monitoring is a question that has been addressed at a number of levels. Auditing Statement 5

(Public Company Accounting Oversight Board 2007) discusses the need to select data that is both timely as well as relevant to the overall internal control evaluation. One approach to the timing issue is the use of continuous monitoring procedures (Alles, Kogan and Vasarhelyi 2004).

Continuous monitoring examines data on an ongoing basis and is particularly suited for those situations in which even a few occurrences of an exception represent a material weakness. The prevention of inappropriate credit card use is such an example. There are many control exceptions that by themselves are not material, but instead need to be reviewed in the context of the entire population of events. If a single person is hired that does not meet the characteristics of the designated employee type or a single order is shipped prior to being approved there might not be a determination that there is a material weakness in internal controls. What if there are two people or two shipments? At some point the evidence of the exceptions becomes overwhelming and there is a determination that a material weakness exists; in general management policy is not being followed. It is the exceptions to managements' policy statements, in the form of the permissions, which correspond to the evidence used in the evaluation decision. Terms like subjective (Rittenberg and Schwieger 2001) and reasonable possibility is Auditing Statement 5 (Public Company Accounting Oversight Board 2007) and reasonable basis for the opinion in Auditing Statement 2 (Public Company Accounting Oversight Board 2007) makes this evaluation a separate issue. However, the permission structure does embody the statements of management policy and therefore the exceptions do support this decision.

Section 6 – Conclusion

The management of a business organization requires the identification of the objectives of the organization and then creating a path by which these objectives can be met. This path includes a number of incremental steps that correspond to states to be achieved. Management must communicate to the employees within the organization the acceptable way in which the activities associated with these steps should be accomplished. The accepted pattern for the performance of these activities corresponds to management policies. To control the organization as it proceeds toward the states in which objectives will be met, management must communicate these policies and review the adherence to them. It can become overwhelming to create these policies on a case by case basis and so a mechanism to establish and represent these policies that is scalable is critical to allow management to run any large organization. These policies can be

viewed in terms of permitting certain types of employees to perform types of activities on certain objects. In order to ensure that the formulation of policy is done at the appropriate level within the organization the span of control and authority must be included in the permission granted to either groups or individual employee types. The delegation of permissions to perform or delegate further down the hierarchy is essential to formulating policy and controlling any large organization. By establishing the roles for each group or type of employee that includes those activities they are allowed to perform or delegate the permission structure represented in this paper again allows management to exercise control at a high level and enforced at the level of granularity considered necessary. The permission structure discussed here extends the REA ontology and allows for this ontology to be directly incorporated into the permissions. By using this ontology as the basis for the different object types in the permissions the semantics of business objects is preserved which allows for the administration of the controls in a way that is psychologically similar to the way in which a manager would specify their policies.

Works Cited

- Ahn, Gail-Joon, and Ravi Sandhu. "Role-Based Authorization Constraints Specification." *ACM Transactions on Information and Systems Security*, 2000: 207-226.
- Baldwin, Robert W. "Naming and Grouping Privileges to Simplify Security Management in Large Databases." *IEEE Computer Society Symposium on Research in Security and Privacy*. Oakland, CA: IEEE Computer Society, 1990. 116-122.
- Committee of Sponsoring Organizations of the Treadway Commission. *Internal Control - Integrated Framework*. Committee Report, Jersey City, NJ: American Institute of Certified Public Accountants, 1994.
- Geerts, Guido, and William E. McCarthy. "Augmented Intensional Reasoning in Knowledge-Based Accounting Systems." *Journal of Information Systems*, 2000: 127-150.
- Geerts, Guido, and William E. McCarthy. "Policy-Level Specifications in REA Enterprise Systems." *Journal of Information Systems*, 2006: 37-63.
- Geerts, Guido, and William E. McCarthy. "Modeling Business Enterprises as Value-Added Process Hierarchies with Resource-Event-Agent Object Templates." In *Business Object Design and Implementation*, by J. Sutherland and D. eds Patel, 94-113. London: Springer-Verlag, 1997.
- ISO15944-4 Information Technology - Business Operational View*. Committee Report, Geneva: International Organization for Standardization, 2007.
- IT Governance Institute. *CoBIT 4.1*. Committee Report, Rolling Meadows, IL: IT Governance Institute, 2007.
- Li, Ninghui, and Ziqing Mao. "Administration in Role-Based Access Control." *ASIACCS'07*. Singapore: ACM, 2007. 127-137.
- Li, Ninghui, Benjamin N. Grosz, and Joan Feigenbaum. "Delegation Logic: A Logic-Based Approach to Distributed Authorization." *ACM Transactions on Information and System Security*, 2003: 1-42.
- Li, Ninghui, Mahesh V. Tripunitara, and Ziad Bisri. "On Mutually Exclusive Roles and Separation-of-Duty." *ACM Transactions on Information and System Security*, 2007: 1-36.
- McCarthy, William E. "The REA Accounting Model: A Generalized Framework for Accounting Systems in a Shared Data Environment." *The Accounting Review*, 1982: 554-578.
- McLean, John. "Security Models and Information Flow." *IEEE Computer Society Symposium on Research in Security and Privacy*. Oakland, CA: IEEE Computer Society, 1990. 180-187.

Nabar, Shubha U., Bhaskara Marthi, Krishnaram Kenthapadi, Nina Mishra, and Rajeev Motwan. "Towards Robustness in Query Auditing." *Proceedings of the 32nd International Conference on Very Large Data Bases*. Seoul, South Korea: ACM Press, 2006. 151-162.

Nash, Michael J., and Keith R. Poland. "Some Conundrums Concerning Separation of Duty." *IEEE Computer Society Symposium on Research in Security and Privacy*. Oakland, CA: IEEE Computer Society, 1990. 201-207.

Porter, Michael. *The Competitive Advantage: Creating and Sustaining Superior Performance*. New York: The Free Press, 1985.

Public Company Accounting Oversight Board. *AUDITING STANDARD No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements*. Bylaws and Rules – Standards – AS2, Public Company Accounting Oversight Board, 2007.

Public Company Accounting Oversight Board. *Auditing Standard No. 5 – An Audit of Internal Control Over Financial Reporting That Is Integrated with An*. Bylaws and Rules – Standards – AS5, Public Company Accounting Oversight Board, 2007.

Rittenberg, Larry E., and Bradley J. Schwieger. *Auditing Concepts for a Changing Environment 3rd edition*. Orlando, FL: Harcourt, 2001.

Shin, Dongwan, Gail-Joon Ahn, Sangrae Cho, and Seunghun Jin. "A Role-Based Infrastructure Management System: Design and Implementation." *Concurrency and Computation: Practice and Experience*, 2004: 1121-1141.

The Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management - Integrated Framework*. Committee Report, Jersey City, NJ: AICPA, 2004.

United States General Laws. *Sarbanes-Oxley Act (SOX)*. Public Law no. 107-204, Washington, DC: Government Printing Office, 2002.

Warmer, Jos, and Anneke Kleppe. *The Object Constraint Language: Precise Modeling with UML*. Reading, MA: Addison Wesley Longman, 1999.

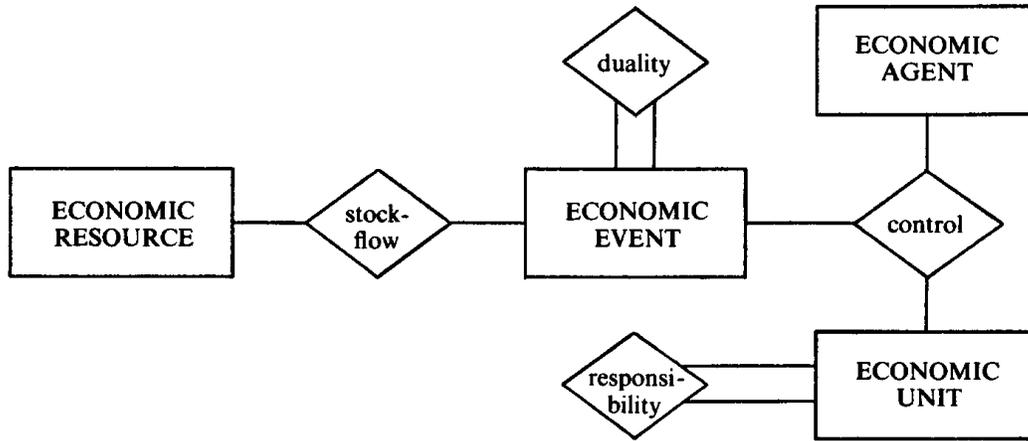


Figure 1- The REA Model (McCarthy 1982)

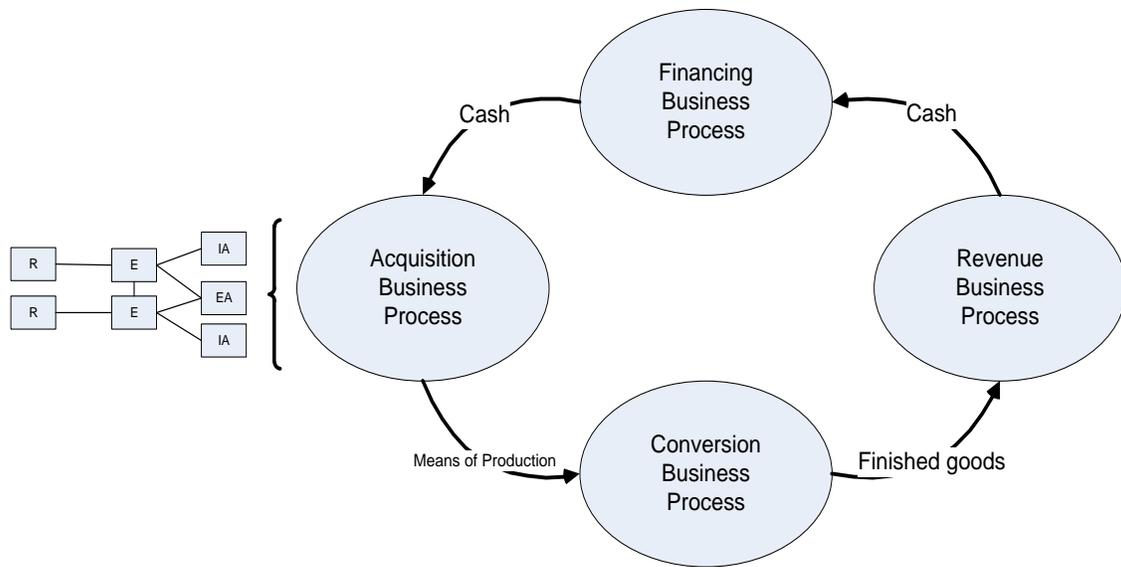


Figure 2 – The Value Chain Model

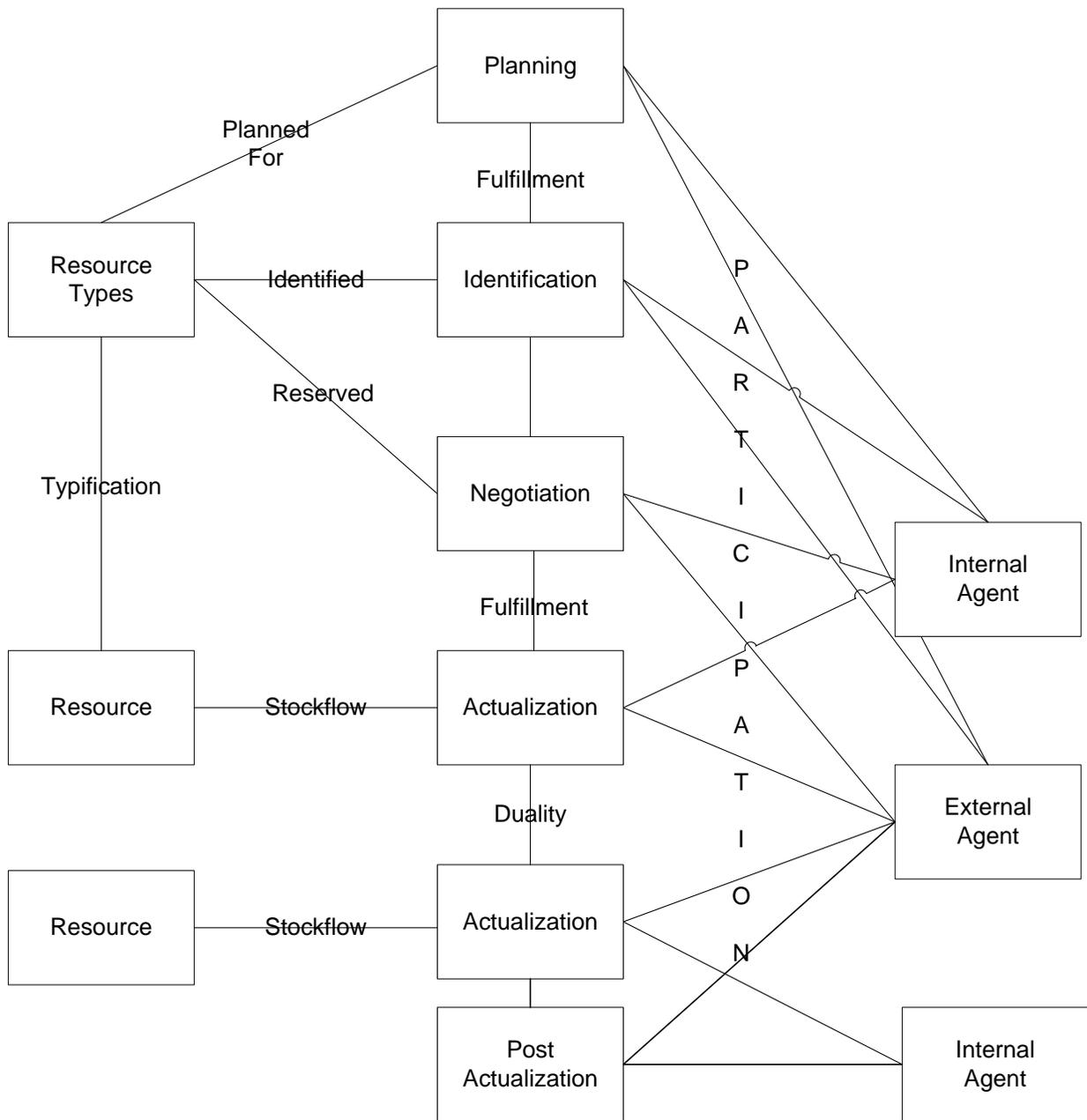


Figure 3 – Extended REA Model – ISO15944

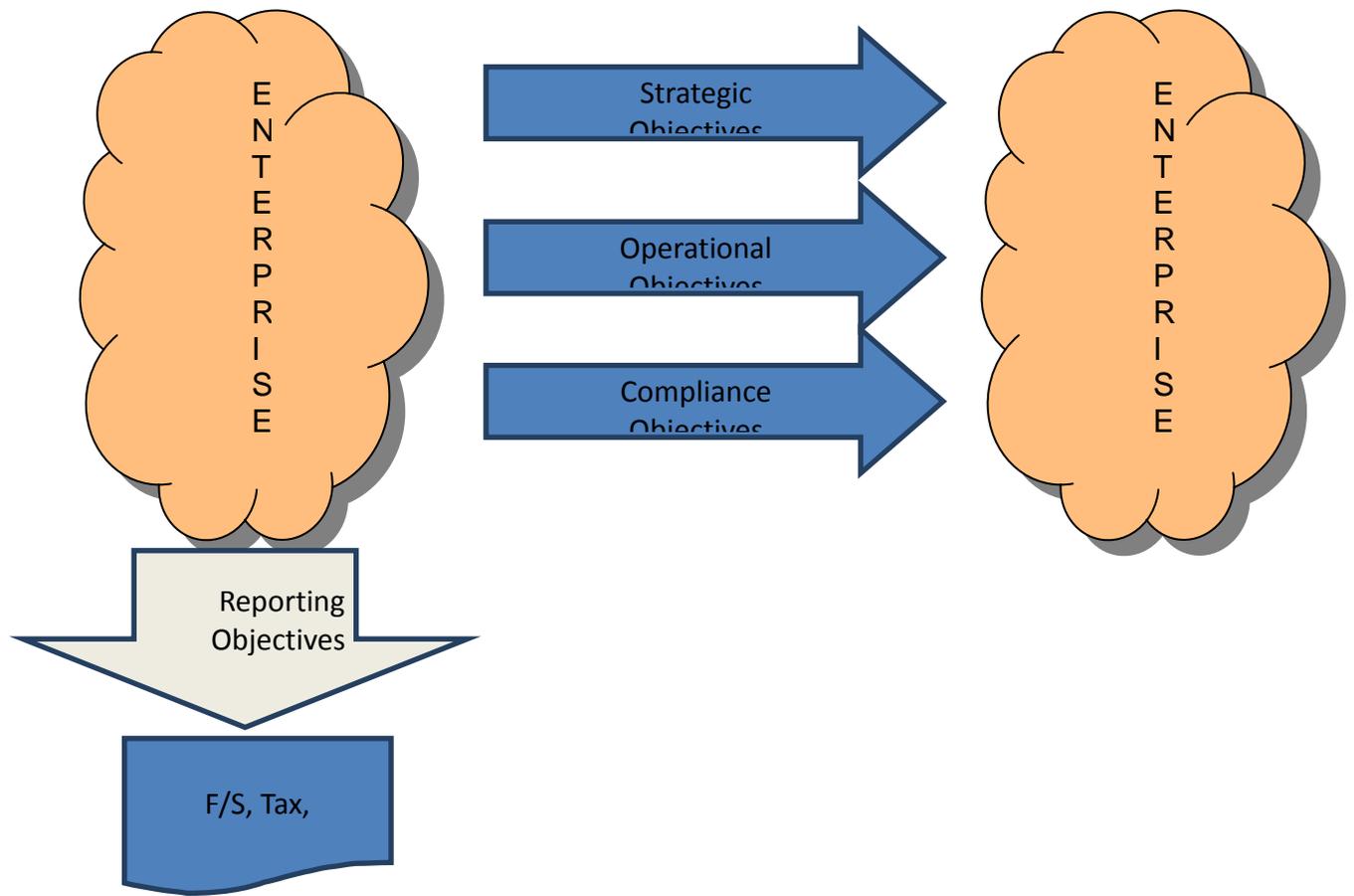


Figure 4 – Relationship of Objectives to States of the Enterprise

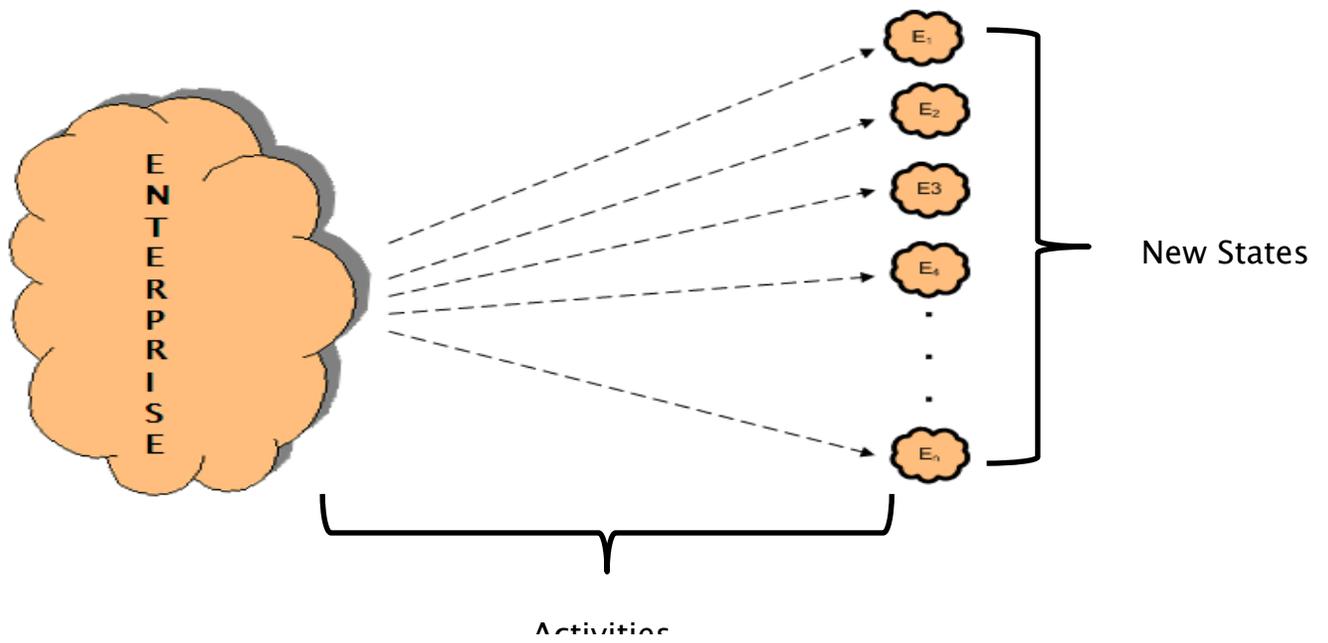


Figure 5 – Activities and Enterprise State Changes

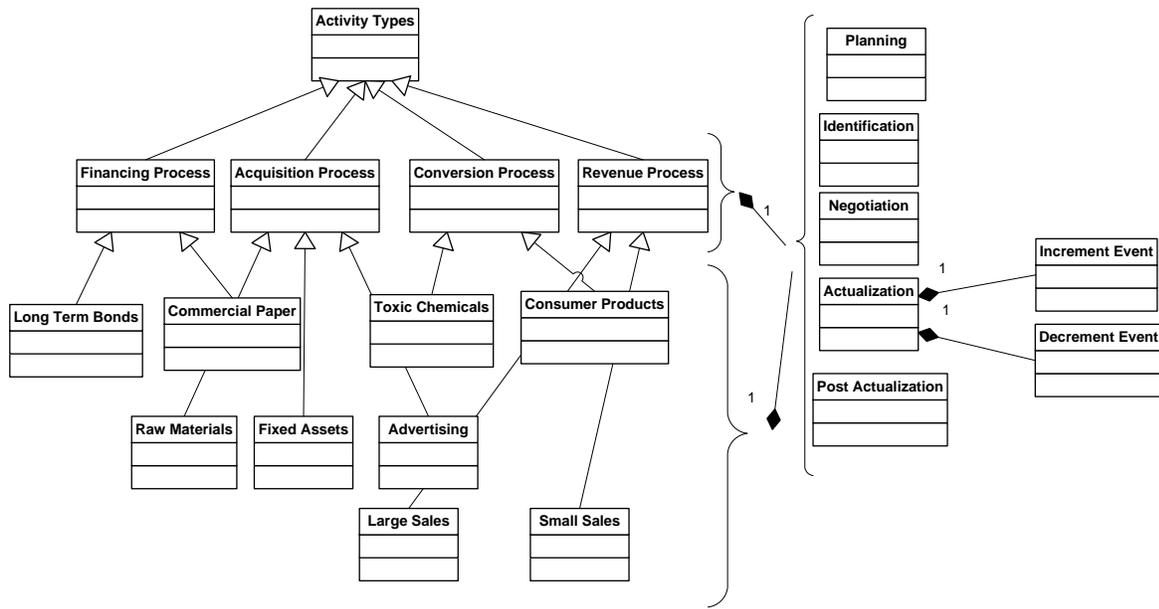


Figure 6a – Activity Type Hierarchy

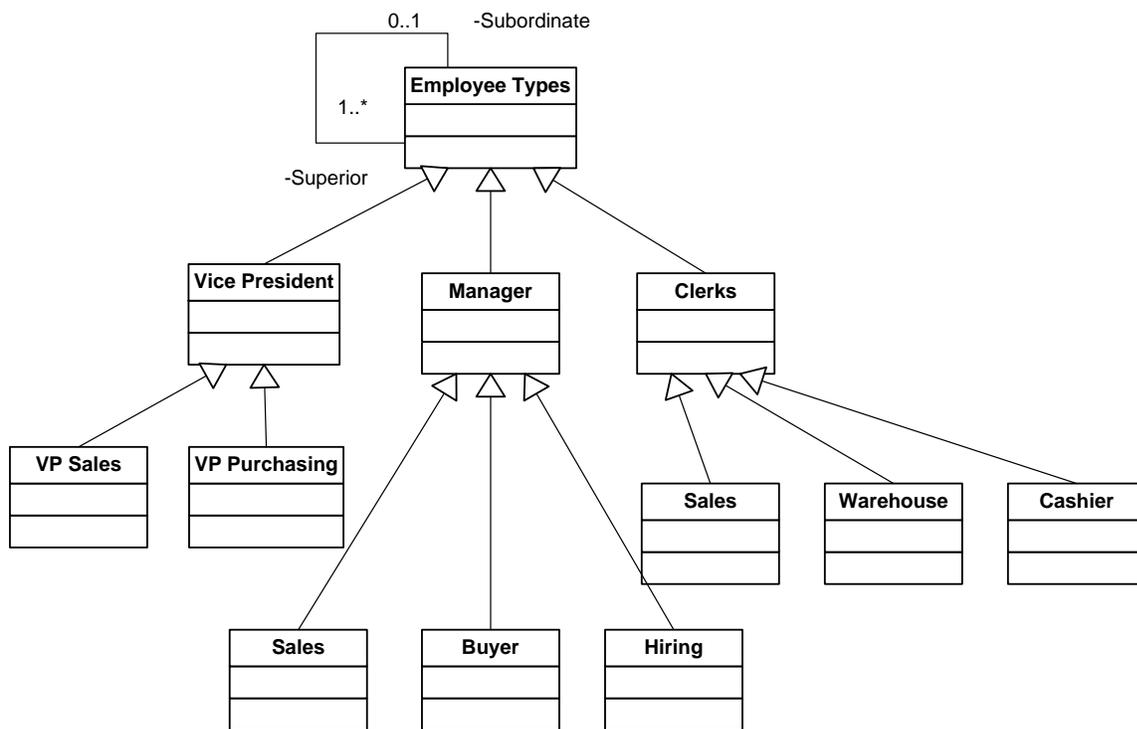


Figure 6b Employee Type Hierarchy

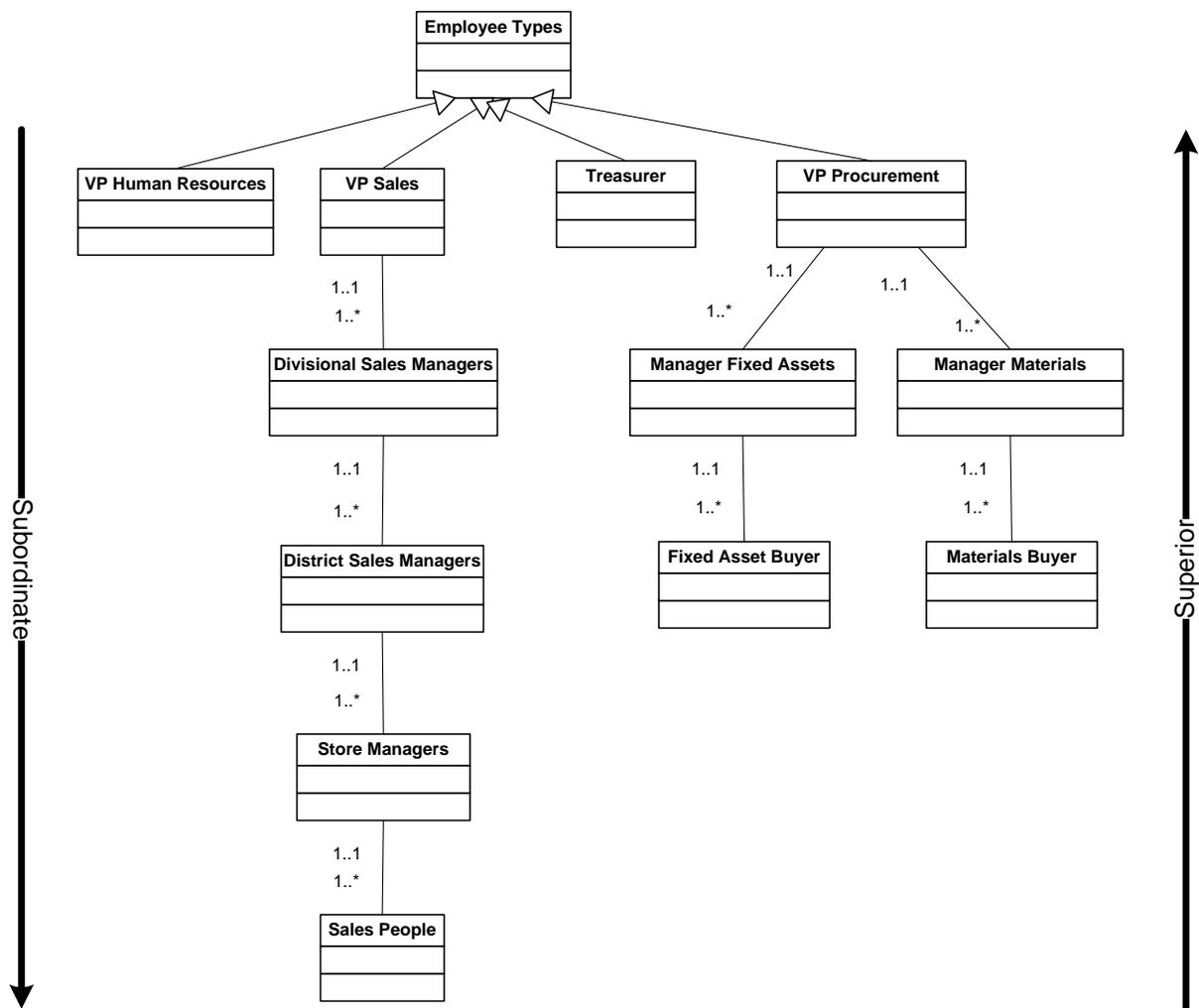


Figure 6c – Employee Types Superior – Subordinate Structure

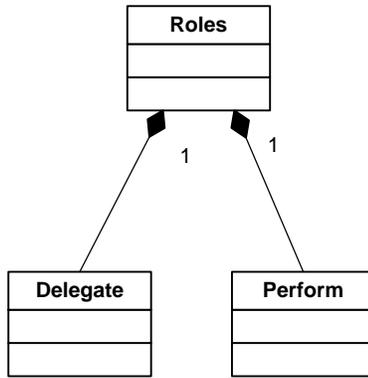


Figure 6d – Role

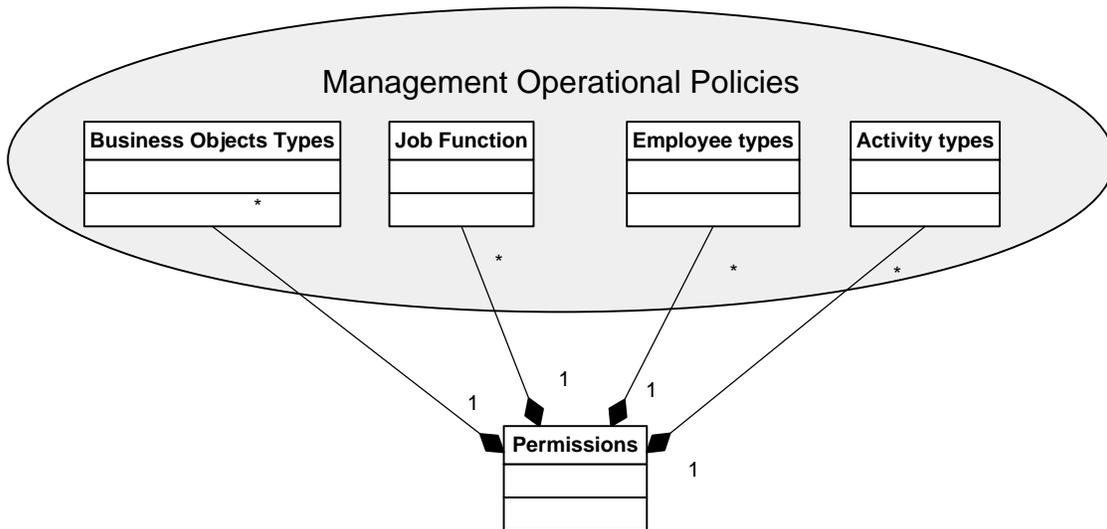


Figure 7 – Basic Structure for Permissions

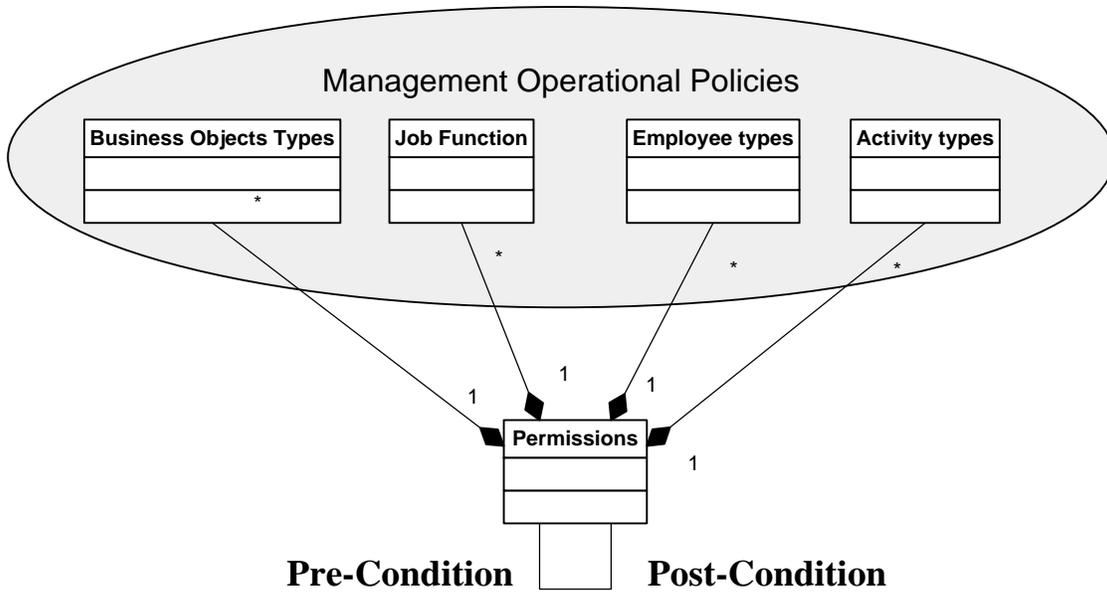


Figure 8- Permissions on Permissions

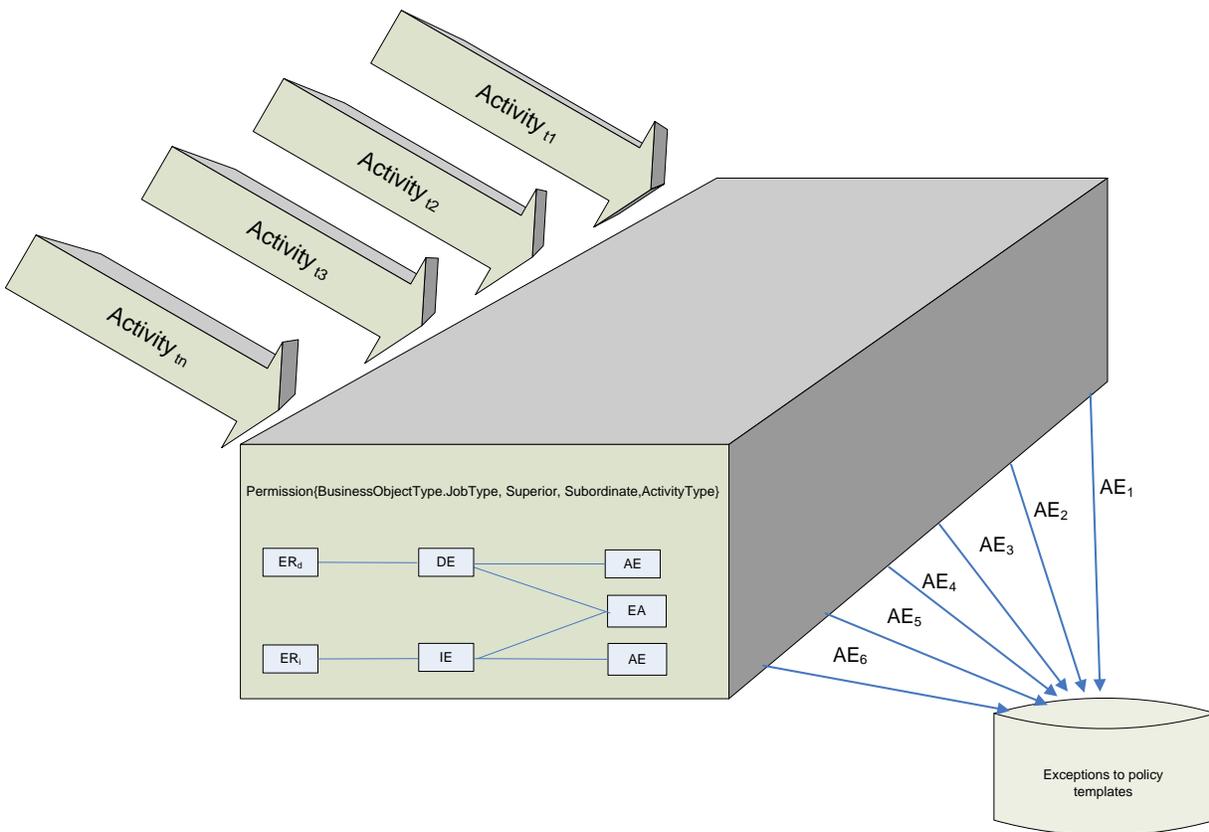


Figure 9 – Continuous Monitoring of Policy Exceptions