Towards Multi-level Organizational Control Framework to Manage the Business Transaction Workarounds

Sérgio Guerreiro
Lusófona University, Campo Grande, 376, 1749-024 Lisbon, Portugal

Keywords: Business Transaction, Control, Framework, Model, Operation, Workaround.

Abstract: Organizations strive to find solutions that perform their business processes more efficiently and effective. Steering the organizational operation using *a priori* prescribed models derives from the classical control engineering theories. These approaches are valid for business information systems domain but require contextual adaptation for dealing with concerns such as change management. In the context of business transaction, the models prescribe the design freedom restrictions for producing a new service or product, and share a common understanding between the stakeholders that have diverse interpretations of it. However, for many and diverse reasons, organizational actors perform workarounds at operation time that could be extremely different from the previous prescribed business transaction models. This paper reviews the organizational control related work and synthesizes it in a conceptual framework. The goal is to establish a set of concepts, and their relationships, to identify workarounds occurring at operation time and then feedback the organizational management with reviewed models, where the control solution encompasses three competence levels: enterprise governance, business rules and access control.

1 INTRODUCTION

Dealing with the issues of efficiency and effectiveness in business transaction operation are cornerstone for a controlled organizational environment. However, due to organizational complexity, the classic control approaches are insufficient because it is impracticable to entire specify the dynamics of the system to be controlled (Herwig, M. & Verelst, J., 2009). To produce decisions about which action to enact, the understanding of the essential dynamic of the enterprise is crucial. Enterprise Ontology (EO) (Dietz, 2006) and the emerging field of Enterprise Engineering (EE) (Dietz et *al.*, 2013) along with dynamic systems control theory (Franklin *et al.*, 2009) are followed in this paper to support the understanding of the business transactions dynamics and the understanding of the workarounds. Theory of workarounds is about how agents with some degree of behavioural discretion decide whether to follow established practices and what to do when exceptions, anomalies and mishaps occur (Alter, in press). Alter S. (2013) states that a workaround is a goal-driven adaptation, improvisation, or other change to one or more aspects of an existing work system in order to achieve a desired level of efficiency, effectiveness, or other organizational or personal goals by overcoming, bypassing, or minimizing the impact of obstacles, exceptions, anomalies, mishaps, established practices, management expectations, or structural constraints that are perceived as preventing that work system or its participants from achieving their goals.

The aim of this novel approach is to integrate a set of concepts that are usually referred alone and that appear to be incompatible. The relationships that exist between the concepts are supported on evidences from the related literature. This conceptual integration allows the design of dynamic systems control applied to the specific context of business transactions operating at run-time. Following this line of thought, whenever a workaround occurs, the organization is aware of it and thereafter it could act with a change in the business transactions models or a change in the access control models. In this paper, we propose a multi-level organizational control framework to manage the business transaction workarounds grounded in the literature review and conceptual synthesis. The following section motivates the need for our study. Thereafter, section 3 includes related

Guerreiro S..
Towards Multi-level Organizational Control Framework to Manage the Business Transaction Workarounds.
DOI: 10.5220/0004870502880294
In *Proceedings of the 16th International Conference on Enterprise Information Systems* (ICEIS-2014), pages 288-294
ISBN: 978-989-758-029-1

work identifying the core concepts for organizational control. Section 4 designs the framework. In the end, the paper concludes the achievements obtained and identifies future work.

2 MOTIVATION

The idea of specifying a framework that is able to cope with workarounds has the wide potential application of offering some new insights to business processes run-time compliance verification and organizational access control models. These following two applications are actually not completely solved. In the first application, the enforcement of Governance Risk and Compliance (GRC) solutions for financial enterprises (Rozinat & van der Aalst, 2008) are demanded by situations such as on May 6, 2010 when the US equity market experienced a severe drop in prices, falling more than 5% in few minutes. In reaction to this, the Securities and Exchange Commission (U.S. Securities, 2010) proposed a rule to pause trading whenever severe drops occur. The decision of pausing in now based in the transaction price of a primary listing market if it moves ten percent or more in the preceding five minutes period. Although the investors view the transaction prices as a single number, it occurs in microseconds and involves executing complex financial processes. GRC observes each micro task of the financial process, within every session, guarantying that the pre-defined governance rules are satisfied; whenever they are not satisfied, it may act pausing the market. In the second application, the organizations need to govern the user's access to their artifacts using fine-grained task-based policies. A lot of solutions are mostly being considered in the technological part regarding security, such as networks protocols, authentication, federated entities, but in practice these solutions are strictly applied to specific enterprise architecture layers (usually the software layers) and do not satisfy the concern of operating in an unified and integrated organizational whole (Nordberg, 2009; DHS, 2013; ENISA, 2013).

In reality, many control systems exist within an organization and many different scientific perspectives are actually available to the manager. Some examples are the access control models (Ferraiolo *et al.*, 2001) that are responsible to grant or revoke the user's access to the different artifacts that exists in an organization. Other example is the business rules that are responsible to maintain the organizational operation within predefined goals (OMG, 2013b). Moreover, in a broader scope, the Enterprise Governance that specifies the design restrictions and the subsequent design for the organizational models (Hoogervorst, 2009).

Also, in the IT industrial context, the efforts presented by the well spread ITIL (OGC, 2011), which is a set of good practices to be applied on infrastructures, operation and maintenance of IT services, shows a solution that prescribes and steers the operation and a continuous change management processes. COBIT (ISACA, 2013) prescribes a framework to enforce IT with control mechanisms, using good practices, policies, procedures, practices and organizational structures. COBIT bridges the gap between business risks, control needs and technical aspects. As the main goal, the undesired events are identified and corrected. Even in the Human body, a multitude of control systems exists, *e.g.*, the Human Peripherical Nervous Systems (PNS) or the Human Central Nervous Systems (CNS).

Therefore, this paper is motivated on this multitude of conceptual definitions pointing to the need of control enforced inside the organization and proposes a multi-level framework applied to the specific problem of controlling the operation of business transaction when workarounds occurs.

3 RELATED WORK

A business transaction is a model representation of a given organizational reality that is valid within a specific timeframe, and that should include who is responsible for each part of the business transaction and the comprehensive definition of system's state and transition (Guerreiro & Tribolet, 2013).

In addition, operation is defined by Dietz (2006) as the collective activity of the elements in the composition and the environment is called the operation of the system. Thus, operation of a system is the manifestation of its construction in the course of time, encompassing both the productions as performed by the elements in the composition and the interactions through the structural bonds. From the perspective of classic control concepts (Franklin *et al.*, 2009) the system that we want to control is the execution of the business transactions. The purpose of a control system is to react whenever the disturbance affects the behavior of the system or whenever a new input is established. By other words, when the system is not producing the desired output for the imposed input. Control act in the input at the same time as the disturbance is affecting the

system.

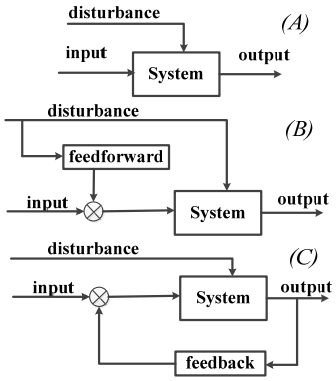

Figure 1: Design pattern of control systems. (A) without control, (B) feed forward control and (C) feedback control.

Figure 1 depicts classical design patterns for a control system. In the top, (A), it shows a system that is not controlled. The disturbance always affects the output delivered by the system. In this pattern, it is not possible to guarantee the behavior of the system output. In the middle, (B), a feed forward pattern that shows that the system input changes accordingly with the actual disturbance. Therefore, the system dynamics it not included in the control actuation. At the bottom of the Figure 1, (C), a feedback control pattern calculates the system input accordingly with the actual misalignment obtained between the output and input. In this pattern, the control actuation calculation takes into consideration the disturbance and the system dynamics. Because the system output depends on the disturbance imposed in the system and on the system dynamics itself. Moreover, to produce results, all systems control requires the capabilities of observation and actuation.

In the scope of a business transaction, observation is the collection of states and transitions whose actors are involved during operation. In fact, there are parts of a business transaction that are observable, while others are unobservable (Guerreiro *et al.*, 2012). Hence, not all the states of the enterprise are controlled. Actuation is the capability to act in the prescribed models.

3.1 Organizational Access Control

Ferraiolo *et al.* (2001) defines that access control, or authorization in its broadest sense, is present in today's every information technology and is concerned with the ways in which users can access resources in the computer system, or informally speaking, with "who can do what". By the authors, access control is arguably the most fundamental and most pervasive security mechanism in use today. The author compares the actual access control models with the Guards, gates and locks that have been used since the ancient times to limit the individual's access to the valuables.

Nevertheless the development of the role-based access control (RBAC) concepts, from the access control models (ACM) community, this approach is only helpful for specifying and implementing the structural security access concerns for a single organizational silo (Ferraiolo *et al.*, 2001). Typically, the ACM follows predefined policies that are applied to a specific application layer of an organization. Examples of such approach are the discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), time-role-based access control (TRBAC), Orcon or Chinese wall (Ferraiolo *et al.*, 2001). Organizational access control models (OACM) are still evolving and are less mature. Concerns related with the access control inside and outside of organizations are identified in the literature (Bertino *et al.*, 1999; Kang *et al.*, 2001). In this security scope, it is also valuable to identify that the 2012 IBM tech trends report (IBM, 2012) points for security as a major adoption barrier and requiring focus beyond IT. The pacesetters organizational actors are establishing security and privacy policies ahead of their peers. IBM defines pacesetters, as the ones that believe emerging technologies are critical to their business success and are using them to enable new operating/business models and that are well ahead of competitors. In this scope, this report recommends a better collaboration between organizations and academia, as well as to develop new strong security and privacy policies to protect the informational assets.

During this research, it has been identified that the solutions offered by ACM scientific community are in most situations decoupled from the detailed organizational artifacts, meaning that organizational access control demands more research efforts.

3.2 Business Rules

A well-known example of low-level business rules implementation is the SBVR language proposed by OMG (2013b). Accordingly, Muehlen and Indulska (2010) explain that separating the process modeling languages and the business rules is not consensual, because sometimes they are complementary in terms of improving the organizational operation. These authors describe the historical evolution of business

rules and investigate the representation capability of Simple Rule Markup Language (SRML), the Semantic Web Rules Language (SWRL), the Production Rule Representation (PRR), and the Semantics of Business Vocabulary and Business Rules (SBVR) specification. A statement that aims to influence or guide behavior and information in an organization defines a business rule. The authors highlight that business rules are a category in that they focus on specifying what is required to take place rather than how something is accomplished. The evaluation uses Bunge–Wand–Weber (BWW) representation theory (Wand & Weber, 1993) and the results show that combining BPMN with SRML provides the highest representation power while suffering an amount of construct overlap that is no higher than that of other language.

3.3 Enterprise Governance

The Enterprise Governance concept is strictly related with the steering concern that exists in many scientific efforts, such as, the General Systems Theory (Bertalanffy, 1969), the Viable System Model (Beer, 1979; Beer, 1981) and the recent Enterprise Governance proposals (Hoogervorst, 2009; Hoogervorst & Dietz, 2008). In general, organizational steering is related with the ability to control, within a bounded effort, the operation of the enterprise towards a desired prescription whenever changes or perturbations occur. In line with this concern, Guerreiro *et al.* (2012) integrates the dynamic systems control (DSC) concepts with the EE concepts to understand, design and implement the enterprise dynamic systems control (EDSC). More recently, in (Guerreiro & Tribolet, 2013) the EDSC solution details the control for the actor's activity, checking workarounds between the prescribed models and the observations. The observed control variables are used to trigger the EDSC. Using the metaphor of CNS and PNS, PNS grounds on the ability to control using a systemic view of the business transactions operations, checking if complies with the ex-ante business transactions and access control models. The result obtained is one low-level control action: *(i)* a grant or revoke access to the activities that are currently attempted and/or *(ii)* a change to the prescribed models. CNS grounds in the ability to control using a systemic view of the historical transactions, checking if complies with the ex-ante business rules. The result is one of the following, high level control actions: *(i)* a change in the business rules, *(ii)* a change in the business transaction model or *(iii)* a change in the access control model. When needed PNS is able to send an order directly to PNS. For instance, new government laws demanding immediate effect. This solution integration allows the design of a non-singular solution, because any set of business transactions designed in any business domain could benefit from this solution, and not only a particular subset of business domains.

4 BUSINESS CONTROL AT OPERATION TIME

This section details a multi-level framework for business transactions control using the concepts defined on literature review.

Figure 2 separates vertically the models from its operation. From one end, models are the prescriptions that the organization wants the actors to follow. When a model is created, changed or deleted we consider that an actuation is being performed. A model is thus actable. On the other end, operation is the collective activity of the various elements in the composition of a system and the environment, therefore when actors workaround then models compliance is not guaranteed. Therefore, operation is observable. This three horizontal layered framework aims at establishing principles that overcome this non-compliance problem, observing what the actors are doing, or attempting to do, and then acting in the business transactions models or in the access control models when needed. Moreover, a workaround is not necessarily harmful for the organization. For instance, if actors are performing differently from the prescription it could indicate new, and innovative, ways of performing their duties (Davison & Ou, 2013).

To facilitate the understanding, and envisioning a future implementation, our framework separates the concepts of observation, actuation and controller throughout different abstraction layers. Regarding the horizontal axis, in the top abstraction layer, the enterprise governance, using feed forward, prescribes models and business rules. It partially follows the definition proposed by Land *et al.* (2009) that state that enterprise governance is the continuous compliance to the rules and is obtained by acting in the model design restrictions that are made available to the governance controllers.

Business rules are established from the feed forward (identified by *Feedforward** in Figure 2) of enterprise governance controller. In the same way,

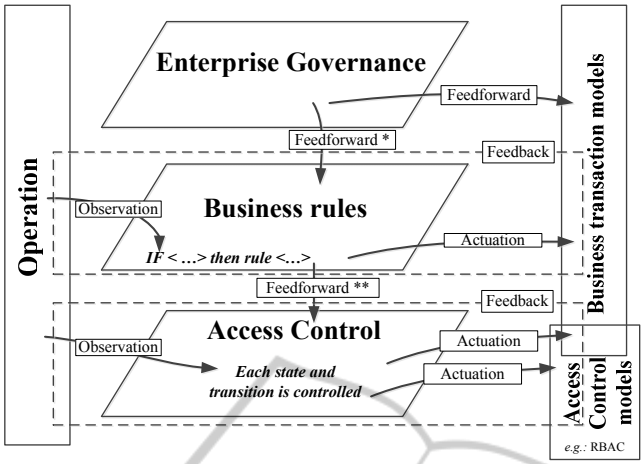

Figure 2: Multi-level organizational control framework. Between different levels feed forward control loops are enforced.

access control are established from the feed forward (identified by *Feedforward*** in Figure 2) of business rules controller. A chain of command and control is thus established between the three layers.

In the second horizontal layer, the business rules are located. In detail, the business rules layer, are a set of production rules of the kind "*if (rule condition) then (rule action)*" that offers the capability to identify if predefined situations occur and then to react, playing an authority role in the organization. A *rule condition* stands for the conjunction of predefined operands and operators taken from the operation, which evaluation results in the logical values *true* or *false*. If a *rule condition* is *true* then a *rule action* is triggered consisting in one of the following executions: *(i)* an *adhoc* action, or *(ii)* a change in the business transaction models (example in Equation 1) or *(iii)* a new feed forward prescription to the access control (example in Equation 2).

if (**actual budget is surpassed**) *then*
Add Auditing transaction (1)

if (**user attempts fraud**) *then*
Revoke all roles from user (2)

Furthermore, the third horizontal layer is devoted to the access control. Many approaches exists for specifying the ACM, here we refer to the example of the well-known RBAC model. ACM focus in the structural dependencies between the different business transactions artifacts and leads to the trustworthiness of the users towards the systems. ACM comprises the principles of responsibility between the organizational actors. RBAC models the concepts for symmetric role-based access control between the concepts of users, roles, permissions and constraints. Users are assigned to a role, and each role has a set of associated permissions. Changing the permissions affects the role and consequently the users associated assigned to that role. These changes are reflected on the access control models.

In detail, on our framework, the access control layer verifies if the operational conditions are conforming to the prescribed access policies. If operation is not conforming to the prescribed access policies then an actuation is enforced on ACM (*e.g.:* revoking user access). Otherwise, if the operational conditions require a change in the business transactions prescriptions, for instance, when a constraint of separation of duties (SoD) is violated then an actuation in the business transaction model is enforced.

Considering the previous definition of a business transaction encompassing the comprehensive description of system's state (*e.g.:* a data store) and transition (*e.g.:* a web service call) a fine-grained access control model is demanded, where each business transaction artifact is strictly enforced with a specific permission. Subsequently, each user is related with a role. The access control is thus able to control if the operational conditions are conforming to the organizational wide access control models, and if not then act in the correspondingly model.

5 CONCLUSIONS

This paper presents a framework for controlling the operation of business transactions. Control cope the workarounds that occur while the organizational actors operate. A workaround is when an actor decide to adapt, improvise, or other change to one or

more aspects of an existing model. In some situations, a workaround could indicate new, and innovative, ways of actors performing their duties. It is not necessarily harmful for the organization.

The control framework separates the operation from the prescribed models, and establishes three horizontal layers: enterprise governance, business rules and access control. The core focus of this framework is studying which are the control concepts and how do they interrelate between each other. The enterprise governance controller sends feed forward information to the business rules and to the business transaction models. By its turn, the business rules and the access controller observe the operation and act in the models. In addition, the integration between RBAC model and business transaction models is discussed. The benefit of such integration is to fine-grain enforce the access policies in the business transactions artifacts. This framework has the advantage of narrowing the design freedom restrictions of the organizational control issue and facilitates the related discussions between peers. Future work will include a comprehensive taxonomic study focusing on the relationship that exists between the workarounds and the business transaction redesigns.

REFERENCES

Alter S., 2013, Theory of Workarounds. Communications of the Association for Information Systems.

Alter, S., 2013. Work System Theory: Overview of Core Concepts, Extensions, and Challenges for the Future, *Journal of the Association for Information Systems*, 14 (2), article 1.

Beer, S., 1979. *The Heart of the Enterprise*, John Wiley & Sons Inc. New York, NY.

Beer, S., 1981. *Brain of the Firm: The Managerial Cybernetics of Organization*. John Wiley & Sons Inc. New York, NY.

Bertalanffy, L., 1969. *General Systems Theory*. George Braziller, New York, NY.

Bertino, E., Ferrari, E., and Atluri, V., 1999. The specification and enforcement of authorization constraints in workflow management systems. *ACM Trans. Inf. Syst. Secur.*, 2(1):65–104.

Davison, R., & Ou, C., 2013. Sharing Knowledge In Technology Deficient Environments: Individual Workarounds Amid Corporate Restrictions. In 21th European Conference on Information Systems, Utrecht.

DHS, 2013. Department of homeland security strategic plan fiscal years 2008-2013. *Homeland Security, USA*, retrieved from http://www.dhs.org.

Dietz, J., 2006. *Enterprise Ontology – Theory and Methodology*. Berlin, Heidelberg, Springer-Verlag.

Dietz, J., Hoogervorst, J., Albani, A., Aveiro, D., Babkin, E., Barjis, J., Caetano, A., Huysmans, P., Iijima, J., van Kervel, S., Mulder, H., Op 't Land, M., Proper, H., Sanz, J., Terlouw, L., Tribolet, J., Verelst, J., & Winter, R., 2013. The discipline of enterprise engineering. *International Journal of Organisational Design and Engineering*, 3 (1), 86-114.

ENISA, 2013. *European network and information security agency*. Retrieved September 20, 2013, from http://www.enisa.europa.eu/.

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., and Chandramouli, R., 2001. Proposed NIST standard for role-based access control. *ACM Trans. Inf. Syst. Secur.*, 4(3):224–274.

Franklin, F., Powell, D., & Emami-Naeini, A., 2009. Feedback control of dynamic systems. 6th ed. Addison-Wesley Publishing Company.

Guerreiro, S., Vasconcelos, A, & Tribolet, J., 2012. Enterprise dynamic systems control enforcement of run-time business transactions. In EEWC 2012, series Lecture Notes in Business Information Processing, volume 110, part 2, Delft, Netherlands pp.46-60.

Guerreiro, S., & Tribolet, J., 2013. Conceptualizing Enterprise Dynamic Systems Control for Run-Time Business Transactions. In *21th European Conference on Information Systems*, Utrecht.

Herwig, M. & Verelst, J. 2009. Normalized Systems: Re-creating Information Technology based on Laws for Software Evolvability. Koppa.

Hoogervorst, J., & Dietz, J., 2008. Enterprise architecture in enterprise engineering. *Enterprise Modelling and Information Systems Architecture*, 3 (1), 3-11.

Hoogervorst, J., 2009. *Enterprise governance and enterprise engineering*. Springer-Verlag.

IBM, 2012. Fast track to the future, IBM Center for Applied Insights, The 2012 IBM Tech Trends Report.

ISACA, 2013. Control Objectives for Information and related Technology, COBIT 5.

Kang, M. H., Park, J. S., and Froscher, J. N., 2001. Access control mechanisms for interorganizational workflow. In SACMAT '01: Proceedings of the *sixth ACM symposium on Access control models and technologies*, pp. 66–74, New York, NY, USA. ACM.

Land, M., Proper, E., Waage, M., Cloo, J., and Steghuis, C., 2009. Enterprise Architecture Creating Value by Informed Governance. Springer-Verlag.

Muehlen, M. & Indulska, M., 2010. Modeling languages for business processes and business rules: A representational analysis. *Information Systems Journal*, 35 (4), 379-390.

Nordberg, T., 2009. Security and trust, the foundation for building an eunion. Paper presented at the Proceedings of the *5th Ministerial eGovernment Conference*, Malmö.

OGC, 2011. Office for Government Commerce, ITIL v3, Information Technology Infrastructure Library.

OMG, 2013. Object management group. Semantics of business vocabulary and business rules. Retrieved from http://www.omg.org/spec/SBVR/1.0/PDF.

Rozinat, A. & van der Aalst, W., 2008. Conformance checking of processes based on monitoring real behavior. *Information Systems Journal*, 33 (1), 64-95.

U.S. Securities, 2010. U.S. security & exchange commission: Preliminary findings regarding market events of may 6. *U.S. Commodity Futures Trading U.S. Securities & Exchange Commission*, 2010.

Wand, Y. & Weber, R., 1993. On the ontological expressiveness of information systems analysis and design grammars, *Information Systems Journal*, 3 (4), 217–237.