# Computational normative approach to SOD risks

Rob Christiaanse, Delft University of Technology,Paul Griffioen, CWI, Joris Hulstijn, Delft University of Technology, Yao-Hua Tan, Delft University of Technology

Keywords: Information integrity, Segregation of duties, internal control

Abstract: Segregation of duties is critical to effective internal control; it reduces the risk of both erroneous and inappropriate actions within and across firm boundaries. Segregation of duties is a deterrent to fraud because it requires collusion with another person to perpetrate a fraudulent act. Segregation of Duties (SOD) is a basic building block of sustainable risk management and internal controls for a business. In this paper we have tested a computational normative approach for analyzing SOD risks in a modern networked organizations from a contractual point of view with real life data concerning taxi-bus transport services for secondary school pupils in the Netherlands, who need to attend special schools. We argue that the complexity of the fraud scenarios can be reduced by means of classifying the nature of the SOD risks in terms of exclusive categories so auditors, risk managers and controllers can actually use scenario outcomes for assessing material risks substantially weakening the internal control system and therefore violating first principles which surely compromises the effectiveness of internal control measures, risk management en audit effectiveness. .

## 1 INTRODUCTION

Sellers and buyers participating in a network depend on each other; they will have to trust one another not to take advantage of each other. In particular, network participants must rely on the data being shared. Segregation of duties is critical to effective internal control; it reduces the risk of both erroneous and inappropriate actions within and across firm boundaries. According to control and auditing theory: no employee should be given too much responsibility over business transactions. The underlying rationale is that an employee who is given a combination of authorization, recording and custody rights may be tempted to commit or conceal fraud (Romney et al 2009, p 243). Without segregation of duties, material weaknesses in the internal control system of an organization, such as e.g. management override, will generally not be detected by management, controller or auditor, as they should according to current regulation (e.g. Sarbanes, Oxley 2002; PCAOB 2007, COSO 2009). Segregation of duties is a deterrent to fraud because it requires collusion with another person to perpetrate a fraudulent act.

When we analyze SOD risks in a modern networked organizations we might ponder about the key question: “how do we know whether all critical SOD requirements buttressing a control system are met ensuring overall effectiveness?”. Manually or at best semi-automated procedures are not feasible because of the complexity of this endeavor. In this paper we use a computational normative approach to information integrity coined as a value net approach tested with real life data. We have modeled iIllicit behavior by adding the worst case state manipulations using insights of. [Els96] and extended the notion of tours by adding a contractual exchange mechanism to the value net representing the valuechain. Hence value nets are process specifications that do not aim at process execution but at process diagnosis and normative analysis. Hence when used in computer science, often the purpose of these models is to analyze the representations of actions and events in a business process, and study their well-formedness. Compare for example the use of the REA ontology [McC82], e3-value [GA03], DEMO [Die06], Supercycle [Els2007] and Model based auditing using REA [ElW2012] . The remainder of the paper is structured as follows.

In Section 2 we present the SOD principles for information integrity. In Section 3 we present the results of an computational normative approach to analyzing SOD risks within the value chain.

.

## 2 PRINCIPLES FOR INTEGRITY

Good management control implies a process, effected by an entity's board of directors, management and other personnel, and designed to provide reasonable assurance regarding the

achievement of objectives in the following categories: (1) effectiveness and efficiency of operations, (2) reliability of financial reporting, and (3) compliance with applicable laws and regulations (COSO 1992/2013). Reliability depends on the way in which data concerning the primary business processes are recorded, processed and stored. In other words, information integrity and in particular reliability depends on the way in which data integrity concerns are reflected in the design and implementation of the (accounting) information systems of the organization.

In essence business reality can be modeled as a value cycle: an interrelated system of flows of goods and money (Starreveld et al 2002). Hence the basic unit of analysis is a contractual relationship hereafter referred to as a transaction. The value cycle of a trading company for example contains two types of transactions: purchasing and selling goods. Figure 1 shows an elementary and a more elaborate example of a value cycle for a trading company. Each event is a transfer of values. In the examples the economic events are a series of buy and sell transactions, but in other cases some transformation can also take place.

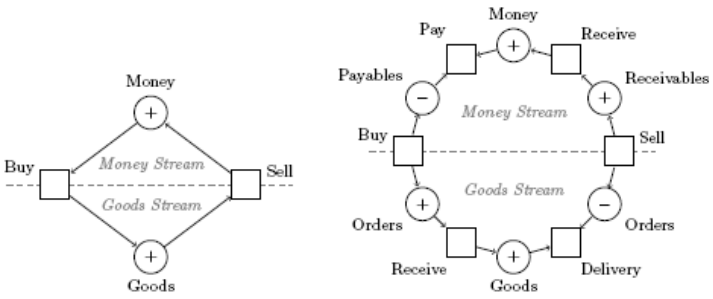


**Fig. 1.** Value Nets for trading companies. The horizontal dashed line splits the model into the *money flow* in the upper part and the *goods flow* in the lower part.

In larger organizations, management has delegated many responsibilities to individuals. Traditionally, responsibilities are separated into three separate roles or functions: the decision making or authorization role, the recording role, and the custody role (Romney and Steinbart 2003). Individuals who make decisions about the commitments of the organization should be authorized to do so, as part of their function profile. In order to have independent evidence, the effects of such decisions should be recorded independently. The recording function is traditionally held by the financial department. Finally, transactions may affect the stored valuables or assets of an organization. Therefore it makes sense to have a separate custody role. Such a role also makes sense in information management: a database manager can be said to have a custodian role, protecting the current state of the database. Reconsider the value cycle as depicted in Figure 2. Segregation of duties is indicated by dotted lines (SoD). As you can see, this results in traditional organizational functions, such as Procurement, Warehousing and Sales.

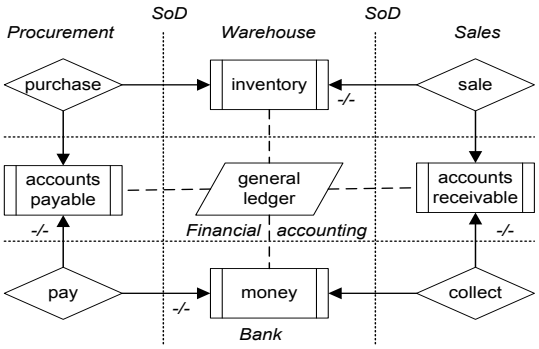


**Figure 2**. Generic value cycle with segregation of duties (Starreveld et al 2002; pp 418).

How does this guarantee that the data in a system will continue to faithfully represent business reality? Messages (receipt, purchasing order; invoice), money and physical goods are exchanged. These messages and flow of goods provide necessary data to be reconciled with the accounts held in the general ledger of the enterprise. For example, the decision to purchase some goods generates a purchase order. A payment is only authorized, when the contents of the invoice

from the vendor correspond to the contents of the purchase order and some evidence of the actual goods (three-way match), for which a receipt is given. Now consider a situation in which the right to authorize payments and the right to initiate purchase orders, or the right to officially receive goods, are given to the same individual. Such a person is in a position to conceal errors or commit fraud, without being detected. Management may even take advantage of such a situation, as in the case of management override. These risks are mitigated (to a certain extend) by allocation decision, custodial and recording rights to different functions within the organization. Segregation of duties ensures that reconciliation relations, like the three-way match, can be used for verification purposes, because there are independent sources of information to be reconciled. When reconciliation checks are built into the information systems, as application controls, this will make it even harder for individuals to make mistakes or commit fraud without being detected.

.

# 3. Computational normative approach for analyzing SOD risk

When we analyze SOD risks in a modern networked organizations we might ponder about the key question: “how do we know whether all critical SOD requirements buttressing a control system are met ensuring overall effectiveness?”. Manually or at best semi-automated procedures are not feasible because of the complexity of this endeavor. We argue that a normative computational approach is both necessary, convenient and efficient for management. In this section we propose a computational approach which enables management, risk managers, auditors to perform and asses risks associated with SOD concerns ensuring informational integrity.

From a computational point of view workflows can be modeled as a value net informally defined as a Petri net with some special characteristics that make it a good representation of the intra and inter organizational processes (structures). For the computation of (normative) behavior in workflows we distinguish monetary units and product units (so the petri net is dimensioned). Hence a value net in monetary units has the advantage that everything is commensurable.

It is possible to specify the normative behavior of value nets and sort out the desirable sequences with the help of the concept of `tour'. A tour relates the behavior of an enterprise to the cyclic structure of its value net i.e. the process model as depicted in figure 1. We want to group transactions that make up what Ijiri calls a causal chain of events [Iji67]. In general terms such a chain of events is a variation on buying products and resources, producing an end product, and selling the product. The cycle starts with the consumption of money and ends with the production of money. A formal notion of the tour concept was introduced for an audit context in [Els96]. It defines a tour as a constellation of events whose total effect is on money only, so all other produced tokens are at some point consumed by another step in the process. Such cyclic behavior follows from the cyclic structure of a business process. In general a value net spans a tour space. A basis for a tour space is a set of tours that spans the space. That means that any tour is a linear combination of (base) tours. Hence a value net is characterized by its tour space. With the unsigned value net we can reveal the various parts of a tour by factoring the tour result, revealing the causal chain. The null space of a value net can be computed, for example with the Fourier-Motzkin algorithm. The resulting tour spaces characterizes the normative behavior of a value net i.e. analyzing for example SOD risks as mentioned in section 2 above.

A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets. The key principle of SOD is based on shared responsibilities of a key (business) process that disperses the critical functions of that process to more than one person or department. Without this separation in key processes, fraud and error risks are far less manageable (AICPA, ISACA) . We have to distinguish fraud from theft from making just an error. Fraud is the undetectable extraction of value from an enterprise. It is a special kind of theft that often involves clever manipulation of an enterprise's assets and liabilities for personal gain. Theft also extracts value, but that will be noticed if an inventory is taken. Fraud is constructed in such a way that the victim does not notice the missing value from the inventory. A good fraud can go on for long periods without being noticed and can form a permanent leak of an enterprise's value. For fraud analysis a value net is extended with journals and illicit actions. A journaling value net adds a journal to each transition to record the event occurrences. Illicit behavior is modeled by adding the worst case state manipulations. [Els96]. Illicit behavior is modeled by transforming each place in the following way:

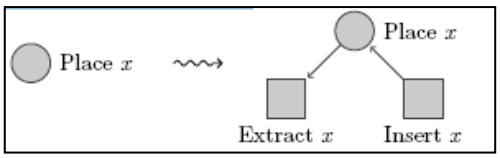


**Figure 3**. Modeling Illicit behavior

Actions Extract x and Insert x are illicit manipulations of the state of Place x. This transformation gives the worst case illicit behavior. Since these actions are added to each place, each state change can be done with them .Performing this transformation after adding the journals immediately gives the ability to manipulate the journals. Note that this transformation must not be performed before adding the journals. Illicit behavior is not recorded in journals.

In 2010 a transport provider has agreed to provide so called taxi-bus transport services for secondary school pupils, who need to attend special schools, which are at a distance. The contract specifies the following revenue model. Based on trip requests (school children travel from A to B at time t, at week day w), the routing sofware package calculates the daily routes at each time of day, and the number of children per route. Remember that that any tour is a linear combination of (base) tours and therefore a value net is characterized by its tour space. As stated by factoring the tour result we can reveal the causal chain. Analogous we can use the price mechanism i.e. the historical agreed upon prices (by means of contractual arrangements between parties) to extend the causal chain across the value chain. It can be shown that historical prices are point symmetric. This is a characteristic ensuring consistency over distributed environments as in networks. The resulting value net is depicted in figure 4.

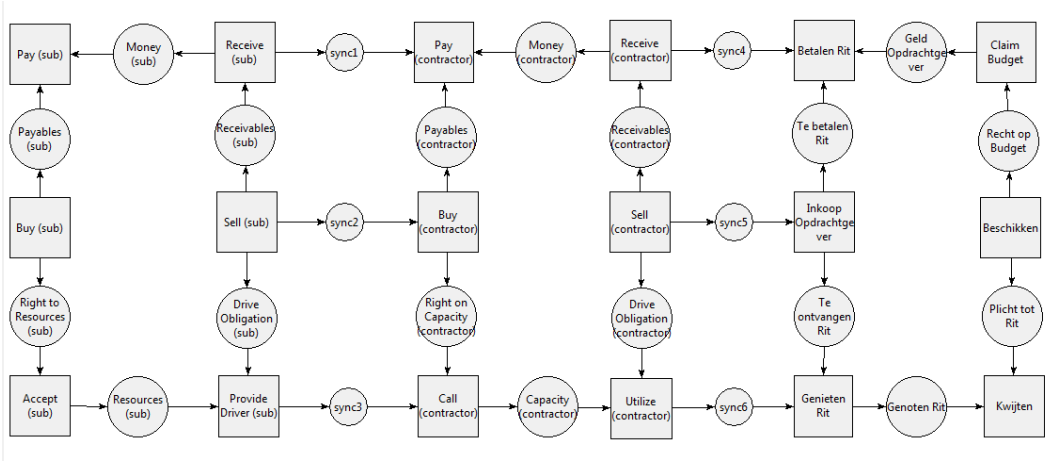


**Figure 4**. Interlinked value nets

Now we can compute all fraud scenario's of the interlinked value nets. The result is that there are theoretically 641 fraud scenario's. The scenarios grow in complexity so it is very hard to decipher whether a scenario should be coined as material or not and how to distinguish type of scenarios. Fraud come in two types, money laundering and money pilfering. Both are illicit but need to be distinguished. So we have to make two models for assessing and categorizing the scenario outcomes. It needs no elaborations that trivial scenarios from definitions need to be excluded from the set of fraud scenario's.

# 5 CONCLUSIONS

We need to be sure, preferably in advance, whether information has been generated according to the applicant procedures and whether it meets organizational standards and regulations. In other words: verifiability and auditability of data processing steps have a major impact on the assurance needed to manage informational risks. Therefore a computational approach only calculating all possible combinations assessing SOD risks does not fulfill the need to be able to assess the strength of internal control systems as designed from a normative point of view. Additionally we need normative models as instantiations of control or audit objectives for assessing and categorizing the scenario outcomes to master complexity form a user point of view.

# REFERENCES


J.E. Boritz (2005) IS practitioners' views on core concepts of information integrity. International Journal of Accounting Information Systems, 6(4):260–279.

COSO (1992) Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission , United States.

COSO (2009) Guidance on Monitoring Internal Control Systems, Committee of Sponsoring Organizations of the Treadway Commission , United States.

J.L.G. Dietz(2006) The deep structure of business processes, Communications of the ACM 49(5): 58 - 64.

J. Gordijn, J.M. Akkermans (2003) Value-Based Requirements Engineering: Exploring Innovative E-commerce Idea. Requirements Engineering Journal, Springer Verlag, 8(2):114-134.

ITGI (2004) Managing Enterprise Information Integrity: Security, Control and Audit Issues, IT Governance Institute.

W.E. McCarthy (1982) The REA Accounting Model: A Generalized Framework for Accounting Systems in a Shared Data Environment, The Accounting Review 57(3) pp. 554-578.

S.M. Welke, W.T. Mayfield, J.E. Roskos (1989) Integrity and Information protection, Report of the international workshop on data integrity, NIST Special Publication 500-168, National Institute of Standards and Technology

PCAOB (2007) Auditing Standard No. 5: An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements, PCAOB Release No. 2007-005A

M.B. Romney, P.J. Steinbart (2009) Accounting Information Systems (11th edition). Prentice Hall, New Jersey.

R.S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman (1996), Role-Based Access Control Models, IEEE Computer, 29(2):38-47.

R.W. Starreveld, O.C. van Leeuwen en H. van Nimwegen (2002) Bestuurlijke Informatie verzorging, Deel 1: Algemene grondslagen (5th edition), Stenfert Kroese, Groningen/Houten (in Dutch).