NEO-CLASSICAL PRINCIPLES FOR INFORMATION INTEGRITY

Rob Christiaanse and Joris Hulstijn

[1] VU University and EFCO Solutions,
[2] Delft University of Technology and Thauris B.V. The Hague
r.christiaanse@efco-solutions.nl, j.hulstijn@tudelft.nl

Abstract: For inter-organizational systems, integrity of information is crucial: how to make sure that the information represented in a system will continue to faithfully represent business reality? In this paper we present a neo-classical approach to information integrity. We apply 'classic' principles of administrative organization and internal control (value cycle; segregation of duties) to a modern network organization. The approach is illustrated with a case study of an e-procurement system for healthcare related transport services. The case illustrates the principles and demonstrates that communication and feedback are crucial for improving and maintaining information integrity.

Keywords: Information integrity, business models, governance and control

1 INTRODUCTION

Out of the three quality aspects of information security, confidentiality, integrity and availability, the aspect of confidentiality gets most of the attention. Indeed potential breaches of information security attract a lot of attention. About integrity of information, however, little has been published. We follow Boritz [1] and define information integrity as representational faithfulness. Information integrity involves both accuracy and completeness and therefore timeliness too, as well as the validity with respect to applicable rules and regulations [1]. Information integrity requires data integrity: "the state that exists when data are unchanged from its source and has not been accidently or maliciously modified, altered or destroyed" [2] p. B26.1. Integrity is closely related to the notion of reliability, see for instance [3].

Under the representational faithfulness view, information must correspond to what is being represented, i.e. business reality. Business reality consists of contractual arrangements between actors, like seller and buyer. In this sense, the idea of a network organization is nothing new: "… most organizations are simply legal fictions which serve as a nexus for a set of contracting relationships among individuals" [4] (p.310). The transactions that enact these contracts are often being constituted by communicative actions, facilitated by an inter-organizational information system [5]. For example, when a purchase order has been issued and confirmed, the buyer has publicly expressed the commitment to purchase goods against a particular price; the seller has expressed the commitment to satisfy this order. Making a commitment has legal and economic consequences, which must be faithfully represented in the (accounting) information systems of buyer and seller.

Sellers and buyers participating in a network depend on each other; they will have to trust one another. To prevent or mitigate opportunistic behavior, inter-organizational governance and control measures are needed [6, 7]. Moreover, parties

are accountable to external stakeholders, like shareholders, or government agencies. These expect evidence that companies are compliant with relevant laws and regulations, as well as corporate guidelines and governance codes (COSO [8], Sarbanes Oxley [9], PCAOB [10]). Therefore, all kinds of controls must be observable and verifiable. Controls can be implemented through incentives, by means of a regulator enforcing the rules, or even better, by hard-wiring control measures into the business processes and information systems themselves, with sufficient evidence. This last approach may be called 'compliance by design' [11].

We will argue that when the 'compliance by design' principle has been properly implemented, automated systems have less traditional risks regarding accuracy and completeness of the reported information. However, the impact of design errors is much larger. The requirements specification and design of the controls to be build into business systems must therefore be explicitly considered. What conceptual frameworks do we have for developing controls, especially for preserving integrity? How can traditional accounts to integrity be adapted to network organizations?

In this paper we present a neo-classical approach to information integrity. The approach is neo-classical, because it is based on classical principles of the value cycle, double entry bookkeeping and administrative organization and internal control [12], while the principles also reflect contemporary business risks, which are often related to communication and decision making in a network organization.

To demonstrate the usefulness and adequacy of the principles, we present a case study about the redesign of an e-procurement system for healthcare transport services. We describe the organization with its contractual partners, and the original problems with reliability of procurement order processing. We show how the principles helped to understand the problems and find a solution. Feedback by means of communication (technology) turned out to be crucial.

The remainder of the paper is structured as follows. In Section 2 we present the neo-classical principles for information integrity. In Section 3 we present the case study to illustrate and motivate the principles.

2 PRINCIPLES FOR INFORMATION INTEGRITY

The purpose of an audit is to reduce the information risk and provide reasonable assurance to some external or internal stakeholder that the financial or other statements reported are reliable, i.e. accurate and complete [13](p 29). But which standards should be used to audit a system's integrity?

2.1 Certifying Transactions: Clark and Wilson

For any information system, the data definition and information structure should follow from the underlying semantics (meaning). The semantics determines which data types make sense, which data values are accepted, and specifies relational constraints between data entries (reconciliation). For example: a date of birth is always prior to the present date, or the total amount of travel expenses aggregated over projects must be equal the total amount of travel expenses aggregated over employees. Such constraints based on the meaning of data are called *integrity constraints*. Integrity constraints can be formalized and automatically maintained by a database management system [14]. Automated enforcement of integrity constraints

requires that users may only access the data through the automated system. This principle of *encapsulation* prevents improper modification.

In Clark and Wilson's model, a so called integrity verification procedure (IVP) verifies whether a data set is well formed, i.e., meets the applicable integrity constraints. A transformation procedure (TP) has two functions. First, for newly entered input data, it verifies whether the data meets the applicable integrity constraints. Second, for all transformations, it will guarantee that the data will remain well formed and integrity constraints are preserved (Figure 1). To make sure that all transactions are well-formed in this sense, all new software must be verified and certified that it does not jeopardize integrity. This explains the high emphasis on change management in modern information security. Without controlling all changes, the well-formedness of transactions can no longer be upheld.

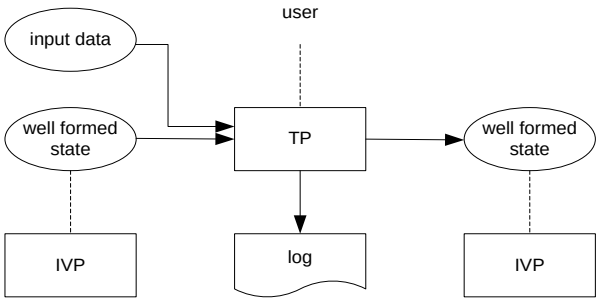

Figure 1. Integrity policies according to Clark and Wilson [15]. Arrows depict information flow and dashed lines depict control.

2.2 Enacting transactions: Communicative acts

At the heart of every business lies the transaction. A transaction (set of contracting relationships among individuals) is an exchange of objects of value, for example money for goods. In order to perform a value transaction, certain operational activities must take place. One could say that the transaction is being represented by these activities. For example, in a cattle market, a deal is represented by slapping hands, payment by handing over cash, and ownership transfer by handing over the cattle. Nowadays, both money and goods may be virtual, but certain communication and operational activities must still be performed. For instance, a user must press [enter] (an action button) in response to a confirmation question or a secret code must be provided. Now the question is: under what circumstances do we have a valid transaction? To use a phrase of Searle [16]: what operational activities *count as* executing a transaction? The answers to this question are coded in inter-organizational systems, and in the procedures and guidelines for human users.

There has been a lot of research on interaction protocols for e-commerce. Here, we take the Language Action Perspective. In particular, we use the Workflow Action loop developed by Weigand and De Moor [17]. All well-formed workflows (interaction protocols), should form a closed loop, consisting of a preparation, a negotiation, an execution and an acceptance phase (Figure 2).

In the preparation phase some agent takes the initiative to generate a commitment. In all cases, some form of explicit confirmation (acceptance) is required. This

exchange of initiatives (request, propose, order) and responses (acknowledgement, acceptance, rejection) is called grounding, because it helps to establish mutual understanding among participants, also called a common ground [18]. In many cases, there will be further negotiation about details of the transaction, including aspects like price, delivery conditions, quality level, etc. Each of these negotiated aspects must again be confirmed. At the agreed delivery time, the performer will then deliver the service. If this is done satisfactorily, the customer will formally accept the transaction, acknowledging that he is now obliged to pay. This is similar to a quittance in accounting theory. Please note that for payment a similar workflow loop is required, but now in reverse. Usually, the preparation and negotiation phases of delivery and payment will be intertwined. Similarly, execution of the payment will count implicit confirmation (acceptance) of delivery.

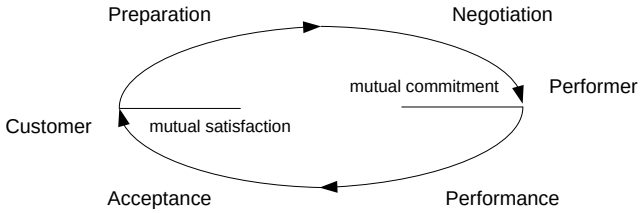

Figure 2. Action Workflow resulting in a transaction [17]

2.2 Recording transactions: the Value Cycle

In essence business reality can be modeled as a value cycle: an interrelated system of flows of money and goods [12]. The value cycle of a trading company for example contains two types of transactions: purchasing and selling goods. The flow of money exactly mirrors the flow of goods, albeit in reverse (Figure 3). We use the following notation. Decisions (authorizations) are indicated by a diamond. An actual decision is an event or change of state. Double rectangles are standard processes, each administering a state of a certain value to the company, such as inventory or accounts payable. States, or more accurately, records of states, i.e. accounts, are related through reconciliation relationships, indicated by dashed lines, which ultimately come together in the general ledger. Data flows are indicated by arrows. The direction of the arrow indicates the influence of events. The sign, '+' or '–/–', indicates an increment or decrement of the corresponding account. Often the '+' sign is omitted. Thus, a purchase leads to an increment of the accounts payable, while the purchased goods are added to the inventory. A sale leads to an increment of the accounts receivable and a decrement of the inventory, etc.

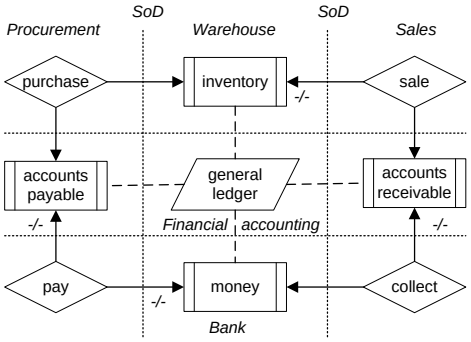

Figure 3. Generic value cycle of a trading company [12]; with segregation of duties.

To make sure no value is lost in the process, an organization (agent, merchant, and enterprise) demands stable reconciliation relationships between certain types of expenses and revenues, assets and liabilities. In a well functioning administration these relationships must always be upheld. Three general rules are applicable:

$$\text{Assets}(t) = \text{Liabilities}(t) + \text{Equity}(t) \quad (1)$$

$$\text{Equity}(t) = \text{Revenue}(p) - \text{Expenses}(p) \quad (2)$$

where ‘t’ denotes a point in time, and ‘p’ is a period ending in t. All alterations in accounts must satisfy

$$\sum \text{Debet} = \sum \text{Credit} \quad (3)$$

For example, if we apply rules (1), (2) and (3) to the value cycle of Figure 1, using the substitution Assets = accounts receivable + money + inventory, Liabilities = accounts payable, Revenue = sales and Expenses = purchases, than we obtain the following derived relationship:

$$\text{Inventory}(t) + \text{Money}(t) + \text{Acc.Receivable}(t) = \text{Acc.Payable}(t) + \text{Revenue}(p) - \text{Expenses}(p) \quad (4)$$

Such relationships can be used to verify accuracy and completeness of records, provided we have independent data sources, i.e. recorded by separate functions.

Given that the sales figure over a certain period p is given by the total value of satisfied customer orders, and that purchases equals the total value of purchase orders, revenue and expenses are built up as follows:

$$\text{Revenue}(p) = \sum_i \text{CustomerOrder}(i)(p) \quad (5)$$

$$\text{Expenses}(p) = \sum_i \text{PurchaseOrder}(i)(p) \quad (6)$$

These last regularities are an example of how the abstract value-cycle is connected to actual communicative actions in an inter-organizational business process. In a similar way, actual payments affect the money in the bank, or purchases affect the inventory.

2.3 Organizing transactions: Segregation of duties

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 custodian role [19]. 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. 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, Warehouse and Sales. But in modern inter-organizational systems, functions need not be static.

In particular, in dynamic RBAC models a role is only defined relative to a session, i.e. an instance of a business process or transaction, with corresponding data and permissions [20]. Roles may be played by different users, and the same user may play different roles, as long as those roles do not conflict concerning the same object, data or process. For example, it is possible that the same person authorizes a sale and a purchase, as long as they concern different goods. In other words: dynamic roles only exist within the scope of a transaction. Therefore organizations can be defined in a much more flexible way, without jeopardizing integrity.

2.4 Ensuring transactions: Compliance by design

In modern enterprise information systems, all steps in the business process are recorded automatically. One could say that the recording function has been taken over by the system. However, this does require a separate system administration function, as now some responsibility for reliable recording is put on systems management.

How does this guarantee that the data in a system will continue to faithfully represent business reality? To explain this, we need to add more detail about evidence of transactions coming from communication (Section 2.1). Imagine a sequence of trading partners in a supply chain, each with a similar structure. This is shown in Figure 3, for a vendor (left) and a client (right). 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 both vendor and client. 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. When such checks are built into the information systems as application controls, this will make it harder to make mistakes or commit fraud without being detected.

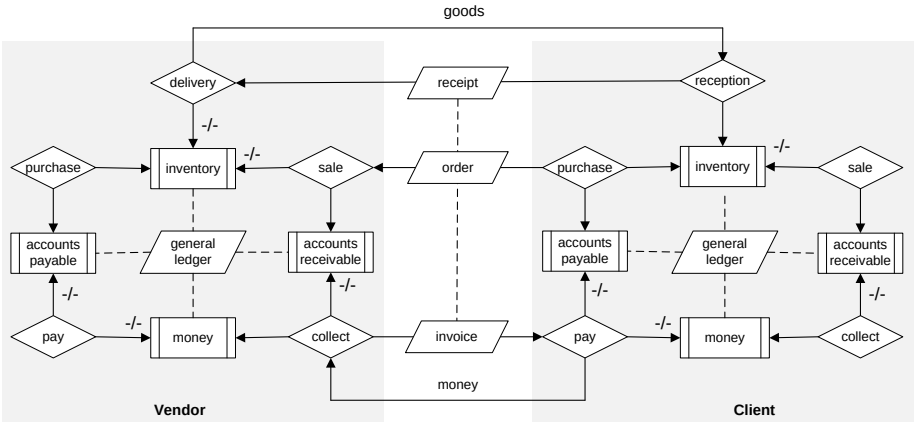

Figure 3. Value cycles of vendor and client with communication and goods.

Application controls and reconciliation controls which are built into the information system are more effective, because they do not only detect misstatements, but they prevent misstatements being made in the first place Compliance concerns the relationship between two sets of specifications: "The normative specifications prescribing what a business has to do and the process modeling specification describing how a business should perform its activities" [11].

3. CASE STUDY: HARTEKAMPGROUP

In this case study we consider the redesign of an integrated information system for procurement of transport services in the health care domain. Because of repeated operational failures and problems with the reliability of financial reporting, management decided for a redesign of the system, based on a preventative approach to information integrity and the reduction of errors.

Data for the case study was collected over a period of several years, by one of the researchers who originally knew the organization in his role of external accountant, and later, as project leader of the information system development project.

Hartekampgroup is a healthcare organization specializing in care and support for people with one or more functional disabilities. Over 1800 clients are serviced on a day to day basis, supported by 1600 employees and 500 volunteers. The service portfolio varies from daycare services, small scale housing communities, ambulant care and specialized crisis support services and activities. The organizational structure is characterized by its divisional form, supported by a small specialized staff.

Many clients are not able to use the public transport system, due to their functional disability. Health care organizations offer transport services on a daily basis, provided that the client possesses a transport permit from the health indication centre. With a permit costs are subsidized under the AWBZ (Exceptional Medical Expenses Act).

In the end of 2002 management within the Hartekampgroup questioned the yearly cost overruns of the transport budget. Management openly questioned the representational faithfulness of the monthly invoice from the transport company. In

the same period the external auditor questioned whether the invoice and the conditions of the contract with the transport company complied with organizational standards and legal demands (AWBZ). Other problems were related to terms of delivery, such as time windows, safety standards, special client demands related to the kind of disability, professional care standards for working with disabled clients and so on. The consequences affected daily routines at the location. Care programs could not start in time, clients were displeased and care personnel questioned the professional quality of the transporting company.

Which factors were causing these problems? To diagnose the problem we used backward chaining using the accounting laws stated in Section 2. The causes which were discovered, then needed be 'repaired' by renegotiation of the contract.

The reasoning is straightforward. A received invoice is considered a faithful representation of reality, when for all trips a three-way-match is possible and the invoiced trips are compliant with the terms of the contract at hand (compare Figure 3). A three way match is only possible when all ordered, performed and invoiced trips are recorded, and all consecutive steps faithfully represent the conditions under which decisions were taken. In other words: when they satisfy the norms of the contract.

The transport services were evaluated against the initial goals and the underlying contract between involved organizations. The following issues were indentified:

I1. *Confirmation*. Conditions under which a trip was ordered and billable were unclear. Transport requests often change due to illness, vacation, change of schedule, address changes, and termination of daycare services. The transport provider must confirm all changes to the schedule. Bad recording practices and lack of confirmation caused disputes about commitments..
I2. *Communication*. The transportation company was badly informed about requested service levels. Specific quality standards must be met (i.e. safety, guidance, specific health conditions). In practice most communication was informal. On location the driver received important preferences related to conditions of a client, such as aggressiveness. These demands can affect schedules and efficiency. Because demands were not recorded, the planning department was making the wrong decisions in reserving transport capacity.
I3. *Compliance*. Invoices did not meet the criteria of applicable rules and regulations. Only clients with a valid transport permit granted by the health insurance indication centre are billable by the transport provider, because only when a permit is granted the transporting costs are subsidized by the government.

All of these problems can be traced back to either information integrity or communication issues. The Hartekampgroup and transport provider agreed that all issues should be addressed in the new five year call-off-contract, including the building of a software application to support the contract and process requirements. In response, the following business and process requirements were formulated:

R1. Client data must be shared among authorized users. Access rights must be aligned with procedures. This requirement meets issues of accountability, here in particular the requirement of separation of duties;
R2. All communication must be instantaneously processed. This requirement meets issues of timeliness;

R3. All communication is part of an agreed upon workflow. This requirement meets issues of repudiation.
R4. All communication must meet the standards of the detailed procedures primarily enlisted in the contract. This requirement meets the integrity issue.
R5. All communications must be traceable. This requirement meets issues of information integrity;
R6. All communications must be verifiable by the consequent authorized user.

A new call-off contract was drawn up, in close collaboration with management, care professionals and the transportation company. Detailed rules and procedures were drawn up to meet organizational standards and regulations. Subsequently the issues I1-I3 were faced and management of the Hartekampgroup and the transport provider decided to implement an integrated internet-based application to improve the communication and registration processes. In addition to an internet based solution for registration and communication purposes, both the Hartekampgroup and the transport provider agreed to discuss registered incidents regularly (i.e. communication feedback from clients, drivers, planning personnel). The results as from June the sixteenth 2003 op till now are quite satisfactorily on both sides.

5 CONCLUSIONS

Information integrity is defined as correspondence to reality. In business, reality is constituted by transactions. A transaction is viewed as a set of contracting relationships among individuals to exchange objects of value, and is represented by a number of communicative acts and operational acts of execution or delivery. Following the language action perspective [17] every workflow needs to close. This means that commitments and performance must be confirmed. When a workflow does not close, for instance because feedback on delivery is missing, the integrity of the information concerning the transaction cannot be assured. These insights about communication and transaction are tightly intertwined with the concept of good management control and the reliability of financial reporting. Information integrity, in particular reliability, depends on the way in which integrity constraints are built into the design and implementation of an (accounting) information system.

In this paper we argue that the classical principles of double entry bookkeeping and administrative organization and internal control, such as segregation of duties, allow reconciliation controls to safeguard assets of an enterprise. We have adopted Starreveld's [12]'value cycle approach and added an language-action account of how communicative actions (orders, confirmations), and operational activities (delivery, payment) connect to the value flow [17]. For example, an invoice is only considered to be a faithful representation of business reality, when a three way match is possible between invoice, order and delivery: the goods or services must conforms to the terms of the contract. This requires that all ordered, invoiced and delivered goods or services are recorded, and all steps of the workflow faithfully represent the conditions under which decisions were taken. As a consequence, auditability and verifiability standards must be simultaneously dealt with!

Although the classical principles about information integrity still apply, we argue that they apply in a different way. In highly automated business environments

traditional static segregation of duties is no longer necessary. Instead, under a dynamic role-based access control scheme, roles only exist in the scope of a transaction [20]. Instead of the traditional three, we distinguish two roles: the decision making or authorizing role and the executing role in combination with a validating mechanism. After all, the recording role has largely been taken over by the system. This does require a separate role of systems maintenance, however.

Our approach can deal with developments in supply chain management, like long tail economics, virtual goods and services, and increased volume and speed of transactions. When there is no external reality against which to verify records, integrity is based solely on validity with respect to procedures. Validity of a transaction is essentially about authorization beforehand and additional verification during and after execution. Such additional checks only work provided the infrastructure provides traceability (audit trail), and the infrastructure supports segregation of duties, by access control tables, personal login and authentication.

Our approach has been illustrated by a case study of the procurement system for transport services in healthcare. The case describes the redesign of the call-off contract, the information systems and communication procedures, in order to improve integrity and legal compliance. The case demonstrates that confirmation and feedback about expected terms and conditions of service delivery are crucial. Also the confirmation procedures for reception of a service need to be clearly defined, so no disputes may arise about invoices and payments. The case shows that compliance should be managed for economic reasons. Benefits are likely to overrun the costs of non-compliance. A traditional detective approach to compliance is too limited; a more preventive approach is necessary: compliance by design [11]. The system will guarantee that information is generated according to standards and regulations.

REFERENCES

1. Boritz, J.E., *IS practitioners' views on core concepts of information integrity.* International Journal of Accounting Information Systems, 2005. **6**(4): p. 260-279.
2. S.M. Welke, W.T. Mayfield, and N.I.o.S.a.T. J.E. Roskos *Integrity and Information protection: Report of the international workshop on data integrity,*. 1989, National Institute of Standards and Technology.
3. Maines, L.A. and J.M. Wahlen, *The Nature of Accounting Information Reliability: Inferences from Archival and Experimental Research.* Accounting Horizons, 2006. **20**(4): p. 399–425.
4. Jensen, M.C. and W.H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure* Journal of Financial Economics, 1979. **3**(4): p. 305-360.
5. Hart, A.P.J. and A.C.S. Saunders, *Emerging electronic partnerships: antecedents and dimensions of EDI use from the supplier's perspective.* Journal Management Information Systems, 1998. **14**(4): p. 87-111.
6. Williamson, O.E., *Transaction Cost Economics: The governance of contractual relations.* Journal of Law and Economics, 1979. **22**: p. 3-61.
7. Bons, R.W.H., R.M. Lee, and R.W. Wagenaar, *Designing Trustworthy Interorganizational Trade Procedures for Open Electronic Commerce.* International Journal of Electronic Commerce, 1998. **2**(3): p. 61-83.

8. COSO, *Guidance on Monitoring Internal Control Systems*. 2009, Committee of Sponsoring Organizations of the Treadway Commission , United States.
9. Sarbanes and Oxley, *Public Law 107 - 204 - Sarbanes-Oxley Act~of~2002*. 2002.
10. PCAOB, *Auditing Standard No. 5: An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements*. 2007.
11. Sadiq, S. and G. Governatori, *The journey to business process compliance*, in *Handbook of Research on Business Process Management*, J. Cardoso and W.M.P. van der Aalst, Editors. 2009, IGI Global. p. 426-454.
12. Starreveld, R.W., B. de Mare, and E. Joels, *Bestuurlijke Informatieverzorging (in Dutch)*. Vol. 1. 1994: Samsom, Alphen aan den Rijn.
13. Knechel, W., S. Salterio, and B. Ballou, *Auditing: Assurance and Risk*. 3 ed. 2007: Thomson Learning, Cincinatti.
14. Grefen, P.W.P.J. and P.M.G. Apers, *Integrity control in relational database systems- An overview.* Data and Knowledge Engineering, 1993. **10**: p. 187-223.
15. Clark, D.D. and D.R. Wilson. *A Comparison of Commercial and Military Computer Security Policies*. in *IEEE Symposium on Security and Privacy*. 1987.
16. Searle, J.R., *The Construction of Social Reality*. 1995: The Free Press.
17. Weigand, H. and A. de Moor, *Workflow analysis with communication norms.* Data and Knowledge Engineering, 2003. **47**(3): p. 349-369.
18. Clark, H.H., *Using Language*. 1996: Cambridge University Press, Cambridge.
19. Romney, M.B. and P.J. Steinbart, *Accounting Information Systems, 10e*. 2006: Prentice Hall, NJ.
20. Botha, R.A. and J.H.P. Eloff, *Separation of duties for access control enforcement in workflow environments.* IBM Systems Journal, 2001. **40**(3): p. 666 - 682.