Organizational Engineering: Support for Internal Control System

Carlos Santos
CEO-INESC / ISCA-UA, Aveiro, Portugal
carlos.santos@isca.ua.pt

Augusta Ferreira
ISCA-UA, Aveiro, Portugal
augusta.ferreira@isca.ua.pt

Carla Ferreira
INESC-INOV, Lisboa, Portugal
carla.ferreira@dei.ist.utl.pt

José Tribolet
CEO-INESC, Lisboa, Portugal
Jose.tribolet@inesc.pt

Abstract

This communication's focus will be on the organizational engineering as a support to internal control system. The implementation of this kind of internal control is essential to promote more dynamic auditing within the organizations. The attention that has been given to internal control has had some effects, i.e., the change of organizational behaviour, from structure to process.

In this paper, we made the extension of the CEO framework, using the "Enterprise Risk Management – Integrated Framework", published in September of 2004 by "Committee of Sponsoring Organizations of the Treadway Commission" (COSO), as a basis to the modelling of internal control mechanisms.

Keywords: internal control system; COSO; CEO Framework; business process

1. Introduction

The trend that has been verified in the evolution of the organizational development (clearly relying on an on-line approach) simultaneously backed by a strong evolution of the communication and information technologies, has confirmed the inefficiency of traditional auditing in assuring the integrity of organizational transactions, making, thus, no sense that these should not be audited in real-time [Onions 2003].

As an equally important factor, we can not forget to mention the change in the pattern of evidences gathering that has been changing over from paper supported documents to digital format [Kanter 2001], which will become the main form of evidences in a near-by future, becoming increasingly important for the good performance of the organizations [Pollitt 2002].

In the last years, with the aim of solving these problems, the issue of real-time auditing has been debated, but this discussion has been restrained to academic circles only. Now, due to constant news of financial scandals, to the market globalization, to the eastern economies liberalization, to the increase in the diversity of working power and to the rising ubiquity of the internet [Julian and Scifres 2002], it is necessary to bring this discussion into practise.

The feasibility of real-time auditing is connected to the existence of an internal control system. Thus, side by side with the strategic and operational aims, control goals should also be supported by adequate processes using adequate resources.

This paper contributes for the promotion of real-time auditing using the CEO framework (CEOF), suggested by the Centre for Organizational Engineering (CEO), research group at INESC-INOV. The CEOF, as verified by several researchers [Aveiro 2002, Castela 2001, Mendes 2001, Sinogas 2002, vasconcelos 2001], is consistent and coherent enough.

Even if the metamodel CEOF suggested by [Sinogas 2002] clearly specifies an association "controls", it is necessary to proceed to its extension, in order for it to support the modelling of internal control mechanisms.

The present communication is divided into five sections, including this one where a brief introduction is made to its aims, context and organization. In section 2 we will do a brief exposition about internal control and its most important frameworks, particularly the "Enterprise Risk Management – Integrated Framework" published in September of 2004 by "Committee of Sponsoring Organizations of the Treadway Commission". Section 3 does an estimation of CEOF on what regards internal control. Section 4 refers real-time auditing, its importance on the developments of the information technologies and the possibility of modelling real-time auditing based on the software agents' technologies. Finally, in section 5, the conclusions and established guiding lines are presented, since the later could be useful in future research projects, related to the topic of real-time auditing.

2. Internal Control

2.1 Concept

It is common to name as internal control system the set of rules, policies and procedures, involved in the management of business risk [Pathak 2003]. These rules, policies and procedures help an operational process to achieve its goal without necessarily being part of the process (see Figure 1) [O'Connel 1999]. These mechanisms are the resources which, if used in an adequate way by the processes, decrease the associated risks.

We say that a control is internal when it corresponds to a mechanism control related to a specific entity. This control can be an excellent tool in order to achieve the organizational goals. However, its implementation should be supported by a coherent and consistent framework [Curtis and Wu 2000].

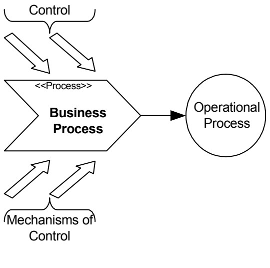

Figure 1 – Processes use external control mechanisms

2.2 Frameworks

An internal control system, when applied with care, judgement and vision, can be the basis of an internal control system that directly supports the success of the organization. If applied mechanically, the consequent internal control system can offer a good control, but not necessarily the organizational success [Galloway 1994].

There are several internal control frameworks [Champlain 1998], usually developed by professional organizations. Six important documents on internal control will be presented next [Colbert and Bowen 2002]:

COBIT – "Control Objectives for Information and Related Technology", published by "Information Systems Audit and Control Foundation", third edition of 2000. It is a framework that offers a tool for the business processes owners, so they can efficiently and effectively fulfil their control responsibilities for the information systems;

SAC – "Systems Auditability and Control", published in 1991 by "Internal Auditors Research Foundation" and revised in 1994. It helps the internal auditors in the control and auditing of technology and information systems;

COSO – "Committee of Sponsoring Organizations of the Treadway Commission", in September of 2004 published the document "Enterprise Risk Management – Integrated Framework" this document include "Internal Control – Integrated Framework", published in 1992. It includes several recommendations as to the best management of how to evaluate the report and improve the control systems;

SAS 55 e 78 – "Statements on Auditing Standards", published accordingly in 1988 and 1995 by the "American Institute of Certified Public Accountants". These give the external auditors a guide on what regards the impact of internal control on planning and executing of businesses process auditing;

CoCo – "Criteria of Control Board – Guidance on Assessing Control – The CoCo Principles", published in June of 1997 by the "The Canadian Institute of Chartered Accountants".

ISO 17799 – "Code of Practice for Information Management", published in 2000 by the "International Organization for Standardization".

Any of the above mentioned models can be used in the design and implementation of an internal control system, without the obligation of using a specific one. However, the COSO framework, besides being the only model that focuses on the entire organization, is also the only one with several references to its universality. It was also as an advantage the fact that it was introduced by the European Committee as a support model for its internal control system. It is also believed by the majority of auditing professionals that an effective control structure under the COSO framework will increase the possibilities of a reliable information system [Moran 2001], one that can be used by the management and by the board, particularly if its control definition is chosen [Hermanson 2003].

2.3 COSO Framework

The "Enterprise Risk Management – Integrated Framework" published by the COSO that include "Internal Control – Integrated Framework" establishes a sequence of events for the management of business processes in control environment [McNamee 1997].

This framework establishes a sequence of events for the enterprise risk management in control environment: (1) Defining the organizations aims; (2) Risk evaluation (identifies it, measures it, prioritize it); (3) Risk Management (controls it, avoids it, and shares it).

It also divides the organizational aims into four categories: (1) Strategic aims, aligned with and supported by the entity's mission; (2) Operational aims, related to the effective and efficient usage of the entity's resources; (3) Reporting aims, related to every organization's needs of internally and externally reporting their performance; (4) Conformity aims, related to the conformity with laws and suitable regulations.

The enterprise risk management is defined as a process, by this framework, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. The eight sub-processes (see figure 2) that constitute it are [COSO 2004]:

Internal Environment – Management sets a philosophy regarding risk and establishes a risk appetite. The internal environment sets the foundation for how risk and control are viewed and addressed by an entity's people. The core of any business is its people – their individual attributes, including integrity, ethical values and competence – and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests;

Objective Setting – Objectives must exist before management can identify events potentially affecting their achievement. Enterprise risk management ensures that management has a process in place to set objectives and that the chosen objectives support and align with the entity's mission/vision and are consistent with the entity's risk appetite;

Event Identification – Potential events that might have an impact on the entity must be identified. Event identification includes identifying factors – internal and external – that influence how potential events may affect strategy implementation and achievement of objectives. It includes distinguishing between potential events that represent risks, those representing opportunities and those that may be both. Management identifies interrelationships between potential events and may categorize events in order to create and reinforce a common risk language across the entity and form a basis for considering events from a portfolio perspective;

Risk Assessment – Identified risks are analyzed in order to form a basis for determining how they should be managed. Risks are associated with related objectives that may be affected. Risks are assessed on both an inherent and a residual basis, and the assessment considers both risk possibility and impact. A range of possible results may be associated with a potential event, and management needs to consider them together;

Risk Response – Management selects an approach or set of actions to align assessed risks with the entity's risk appetite, in the context of the strategy and objectives. Personnel identify and evaluate possible responses to risks, including avoiding, accepting, reducing and sharing risk;

Control Activities – Policies and procedures are established and executed to help ensure that the risk responses management selected are effectively carried out;

Information and communication – Relevant information is identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information is needed at all levels of an entity for identifying, assessing and responding to risk. Effective communication also must occur in a broader sense, flowing down, across and up the entity. Personnel need to receive clear communications regarding their role and responsibilities;

Monitoring – The entire enterprise risk management process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant. Monitoring is accomplished through ongoing management activities, separate evaluations of the enterprise risk management process or a combination of the two.

The COSO framework can only be seen as truly effective when all of its eight components, above identified, are present and correctly functioning (see Figure 2).

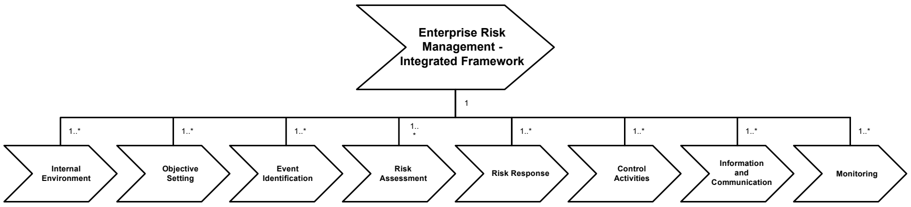

Figure 2 – Enterprise Risk Management - Integrated Framework

3. The CEO Framework and the Internal Control

The CEOF, if given the adequate stereotypes, can support the modelling of internal control, simultaneously with the business modelling, assuring thus the alignment of the internal control system with the business.

A control mechanism of a business process is a consumed resource, used, produced or refined by a control process. These resources, when correctly related to the business processes, main or of support, give the organization's manager the guarantee of achieving with some certainty his/hers business objectives.

3.1 CEO Framework Extension

In order for the metamodel of the original CEOF [Sinogas 2002], to support the "Enterprise Risk Management – Integrated Framework", it is necessary to extend its notation.

In the extension now suggested, there are no changes of the business objectives as seen in the notation studied by [Sinogas 2002], which will continue being the objectives, processes, resources and systems. However, it is suggested that the pre-defined classes of the objectives, processes and resources be revised according to what is next shown.

3.1.1 Aims

- **Semantic** – the objectives determine and ***control*** the business' behaviour and reveal the desirable stages of some business resources.
- **Restrictions** – each objective should correspond to, at least, one process.
- **Graphic Notation** – the graphic notation of the objective uses the icon described (see figure 3) to portray the stereotyped goal <<goal>>.

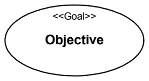

Figure 3 – Graphic notation of the goal

- **Pre-defined Classes** – a strategic objective is composed by operational and control objectives [Weigand and Moor 2001]. The operational aims are specialized in quantitative and qualitative aims. The introduction of control objectives specialized in diverse specific objectives (see figure 4) is done, simultaneously, with the definition of the operational objectives, in harmony with the good established practises or depending upon the organization's own characteristics.

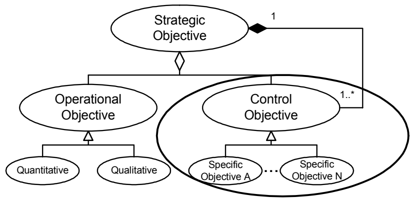

Figure 4 – Pre-defined objectives' classes

3.1.2 Processes

- **Semantic** – a process represents a unity of work and its own execution can be related to the execution of others through resources' flow.
- **Restrictions** – a process should correspond to one or more objectives.
- **Graphic Notation** – the graphic notation for "process" uses the icon described (see figure 5) to portray the process stereotype <<process>>.

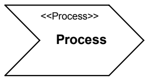

Figure 5 – Graphic Notation of the process

- **Pre-defined classes** – the activities of a business can be classified as main activities, support activities and control activities. The main and support activities depend on the type of business and they change, obviously, according to the type of business. The control activities are necessary to assure that the main or support activities are executed on good terms. These activities should always consider the necessary support to the good execution of the business process (see figure 6).

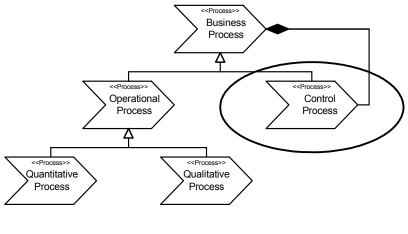

Figure 6 – Pre-defined processes' classes

3.1.3 Resources

- **Semantic** – The resources are business objects, manipulated through processes. They can be arranged or structured and have relations among themselves. They can also be produced, consumed, used or refinished by the processes.

- **Restrictions** – a resource has to be produced, consumed, used and refined in, at least, one process.
- **Graphic Notation** – the graphic notation for “resource” uses the icon shown (see figure 7) to portray the stereotyped resource <<resource>>.

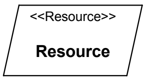

Figure 7 – Graphic Notation of Resource

- **Pre-defined Classes** – The business resources of an organization can either be operational or control ones. The operational resources can be things or information and divide themselves into physical and abstract. A specific class of the physical resource is people or entity (see figure 8). The control resources are defined in function of the risk assessment done to the operational business processes and the systems supported by those.

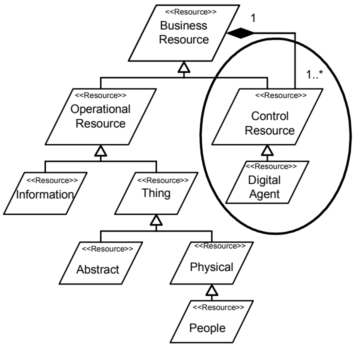

Figure 8 – Pre-defined resources’ classes

4. Metamodel of the Evolution of the CEO Framework

Figure 9 portrays the CEOF’s metamodel evolution. It is clear that the only change introduced, when comparing it with the original CEOF metamodel, consists of the introduction of the association “controls” between “resource” and “system”.

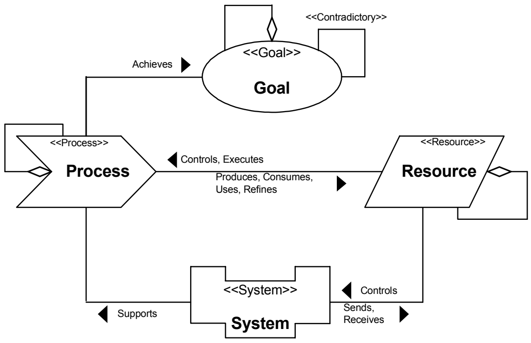

Figure 9 – Metamodel of the framework CEO's Evolution

5. Conclusions and Future Work

This work has given positive indications on what regards the use of the CEOF in the internal control system's modelling, with the help of software agents implementations. In order for this to happen slight changes to its original metamodel are needed.

Using the theory of internal control and the "Enterprise Risk Management – Integrated Framework" published by the COSO, we suggest an evolution of the CEOF, so that, in any modelling process of a business, eventual control mechanisms are identified, or their implementation made possible. The extended CEOF metamodel brings only minimal changes to the original CEOF metamodel.

Lastly knowing that all that has been said is a mere contribute, and knowing that there is still a long path to be walked to achieve the effective and coherent modelling of the internal control in an organization; we suggest as future work the use of the extended CEOF metamodel in modelling business processes, main and support, in real situation.

Studies that theoretically strengthen the process guided real-time auditing model, here suggested should be developed, so as to provide answers to all organizations which are interested in maintaining the integrity of their transactions.

The real-time auditing systems massification depends on its feasibility, according to three topics; technological, economic and cultural:

- **Technological** – the approach is possible, since all transactions, done by an organization, are recorded and stored electronically;
- **Economic** – there may be some problems. This is a question that should be thoroughly analysed;
- **Cultural** – it is necessary that organizations recognize the importance of real-time auditing breaking several organizational taboos, thus receiving important advantages.

Simultaneously, it is also necessary to continue the development of adequate arguments that should give answer to a set of vital questions, related to:

- Real-time auditing architecture;
- Factors that can influence the use of real-time auditing;
- Main consequences of real-time auditing.

6. References

Aveiro, D. 'Organização da Função Informática', Universidade Técnica de Lisboa, 2002.

Castela, N. 'Recolha, Análise e Validação de Informação para Modelação de Processos de Negócio', Universidade Técnica de Lisboa, 2001.

Champlain, J., *Auditing Information Systems: A Comprehensive Reference Guide* (Somerset, New Jersey, 1998).

Colbert, J. L. and Bowen, P. L. 2002. A Comparison of Internal Controls: Cobit, Sac, Coso and Sas 55/78. In, Information Systems Audit and Control Association, http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=8174&TEMPLATE=/ContentManagement/ContentDisplay.cfm. (accessed 2004).

COSO 'Enterprise Risk Management - Integrated Framework' (2004).

Curtis, M. B. and Wu, F. H. 'The Components of a Comprehensive Framework of Internal Control', *CPA Journal* (2000).

Galloway, D. J. 'Control Models in Perspective', *The Internal Auditor* 51, no. 6 (1994), pp. 46-52.

Hermanson, H. M. 'Coso: More Relevant Now Than Ever', *Internal Auditing* 18, no. 4 (2003).

Julian, S. D. and Scifres, E. 'An Interpretive Perspective on the Role of Strategic Control in Triggering Strategic Change', *Journal of Business Strategies* 19, no. 2 (2002), pp. 141-159.

Kanter, H. A. 'Systems Auditing in a Paperless Environment', *Ohio CPA Journal* 60, no. 1 (2001), pp. 43-47.

McNamee, D. 'Risk-Based Auditing', *Internal Auditor* 54 (1997), pp. 22-27.

Mendes, R. 'Modelação de Estratégia de Negócio: Representação, Alinhamento e Operacionalização', Universidade Técnica de Lisboa, 2001.

Moran, J. 'Applying Best Practice Internal Control in the European Commission', *Accountancy Ireland* (2001).

O'Connel, P. 'Internal Control Standards', 1999.

Onions, R. L. 'Towards a Paradigm for Continuous Auditing', 2003.

Pathak, J. 'Internal Audit and E-Commerce Controls', *Internal Auditing* 18, no. 2 (2003), pp. 30-34.

Pollitt, M. M. 'The Very Brief History of Digital Evidence Standards', Paper presented at the Fifth Working Conference on Integrity and Internal Control in Information Systems (IICIS), Bonn, Germany, 11-12 November 2002.

Sinogas, P. 'Modelação de Processos de Negócio', Universidade Técnica de Lisboa, 2002.

vasconcelos, A. 'Arquitectura de Sistemas de Informação no Contexto do Negócio', Universidade Técnica de Lisboa, 2001.

Weigand, H. and Moor, A. d. 'A Framework for the Normative Analysis of Workflow Loops', Paper presented at the Sixth International Workshop on the Language-Action Perspective on Communication Modelling (LAP 2001), Montreal, Canada, 21-22 2001.