THE IMPACT OF E-COMMERCE ON THE INTERNAL CONTROL AND ON AUDITING PRACTICES

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

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

ABSTRACT

The trend that one has verified in Electronic Commerce, assuming the internet as a privileged way for the implementation of inter-organizational communication channels, and also the major development verified in the intra-organizational technological infrastructures (intranets and extranets), have given else to complex commercial partnerships. This complexity has had an enormous impact on what regards internal control systems and auditing practises.

An internal control system is composed by a set of control mechanisms thought of according to the risk management connected to business' processes. These mechanisms play an important role in assuring that electronic commercial transactions are trustful and, so, enabling their increase.

The growing importance of Electronic Commerce and the need to assure the necessary trust in electronic commercial transactions, has led the authors to study and propose, using organizational engineering, an internal control system, from an holistic perspective, thus enabling the implementation of real time auditing practises, of the electronic commercial transactions, using the digital agents' technology.

The authors have chosen, on what concerns the organizational aspects, the OEC framework, suggested by the Organizational Engineering Centre of the INESC-INOV, based on the definition of three main concepts (business strategy, business process and information systems), which technically resorts to the creation at a new profile for the UML language. On the other hand, on what concerns the internal control perspective, the authors have chosen the COSO framework (Committee of Sponsoring of the Treadway Commission), named "Enterprise Risk Management Framework", which approaches the internal control as a process and has a global vision of the organization.

KEYWORD

E-commerce, internal control, business processes, electronic commercial transaction, risk based auditing, real time auditing.

1. INTRODUCTION

The interconnection of network computers, trough the internet, has enabled new forms of electronic commercial transactions, knowing that the prosperity of the 90s is mainly due to the improvements in the information technology and in network computers and not due to the improvement in the production efficiency and products distribution (Smith 1999). The interconnection of network computers, besides the advantages above mentioned, brought along new risks that should be dealt with considering the risk desire underlying each organization. This aim is achieved by risk management. In order for this to happen, specific frameworks can be used, namely the one suggested by COSO (Committee of Sponsoring of the Treadway Commission), called "Enterprise Risk Management Framework".

The evolution that one can see in e-commerce, with the internet playing the main role as the best way to implement information and communication channels, to make the electronic transactions more effective, linking extranets and extending intranets to a commercial partnership environment (Plavsic, Dippel et al. 1999), has produced impact on what regards internal control.

According to the specific characteristics of the Internet, the path taken by a transaction is not easily predictable nor is it possible to assure the security of all systems that participate in an electronic commercial transaction performance. Taking in consideration what has been said above, it is impossible to guarantee a safe electronic commercial transaction environment, by using only technological components (firewalls, for instance), (Plavsic, Dippel et al. 1999). Therefore, we have to conclude the need for the implementation of risk based internal control systems, which take in consideration the new internal control pattern, when commercial transactions are to be made electronically, in an environment that hasn't got the traditional paper support, responsible for the traditional auditing tracks.

The competitiveness, dynamism and complexity of the new digital market have led organizations to guide their businesses in a business guided process perspective. This trend has partially created new demands in the management of the information systems control, which support the business processes (Andersson and Nilsson 1997).

The e-commerce has profoundly changed the market models, leading to the adoption of new rules and to the change in trust from one that was based on people to one that is now based on technology. This change of pattern requires some changes in the traditional control mechanisms (confidentiality, integrity and availability) to a public network with the Internet characteristics (Powell 2000).

Our aim with this paper is to contribute to the development of an internal control model, based on risk, which will enable the feasibility of real time e-commerce auditing systems, using software agents. In order to achieve this, it is necessary to incorporate models, already studied by ourselves in the investigation centre of which we are part.

2. E-COMMERCE

In this paper we shall consider that e-commerce consists of the act of rendering effective a commercial transaction, one that links two entities (customer and supplier), using the Internet as a technological platform to establish the information and communication channel between those two entities. An electronic commercial transaction has the same significance as the traditional commercial transaction, consisting of the satisfaction of a set of needs in exchange of equal value (Kornelius 1999), with the difference of using new communication and information technologies to make itself effective.

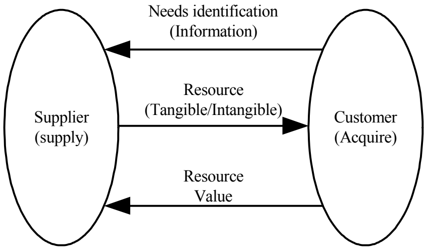

Figure 1. A commercial transaction consists of the satisfaction of a set of needs in exchange of an equal value.

When two entities establish electronic commercial transactions among themselves, their information systems, plus the business processes that each of the entities perform separately, are no longer isolated, obviously. This is the result of the influence that each of the information systems and business processes of one of the entities has over its congeners of the other entity. Simultaneously, the systems that ender effective a channel of communication and information among two entities no longer function separately, working instead with the systems and internal business processes of each of the intervening entities.

Besides what has been previously mentioned, every commercial transaction, both in the traditional format or performed using electronic mechanisms should contemplate the following items:

- **Authentication** - guarantee of the legal entity, singular or plural, with whom we are working;
- **Integrity** - guarantee that the contents of the communication between both parts is not modified;
- **Confidentiality** - guarantee that no one, non-authorized, either intentionally or not, has access to the contents of the communication.

In order to overcome some of the limitations that hold back the development of e-commerce, effective and trustworthy mechanisms are required, to assure the transactions' privacy and security (ANACOM 2004). It is our opinion that these mechanisms can be assured trough the implementation of a risk based internal control system, capable of dealing with the electronic commercial transactions characteristics. This internal control system should contemplate both the intra-organizational controls and the inter-organizational ones, connected to the rendering effective of the traditional commercial transactions.

3. INTERNAL CONTROL

It is commonly designated by internal control system the set of rules, policies and procedures (control mechanisms), involved in the management of business risk (Pathak 2003).

A control mechanism helps an operational process to reach its aim without being, necessarily, part of the process, figure 2 (O'Connel 1999). These mechanisms are resources that, if used adequately by the processes, perform the management of the risks associated to the processes and systems.

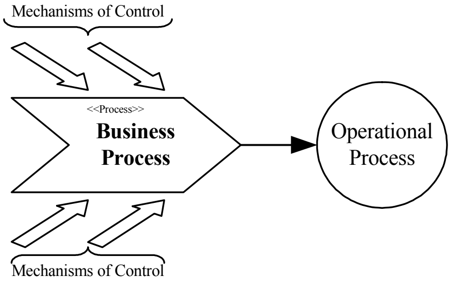

Figure 2. The main business and support processes use control mechanisms external to the process.

One says that a control is internal when it corresponds to a mechanism specifically connected to an entity or negotiated by two or more entities for common usage. This control can be an excellent tool to achieve an organization aims. However, its implementation should be supported by a coherent and consistent framework (Curtis and Wu 2000).

The open nature of the internet makes the entities, involved in internet based electronic commercial process, vulnerable to intentional or no-intentional attacks. Thus, the implementation of internal control systems is vital, which will have as an aim the management of the inherent risks to inter-organizational systems that support real-time electronic transactions (Pathak 2003), based on the Net.

The implementation of an inter-organizational control system is not common, due to the inexistence of a manager of the internet, which would establish the universal laws to be equally applied by all intervening entities. The potential existence of such one entity would largely restrain the creativity of the Net users, which gives the Net its incredible richness.

The single nature of electronic commercial transactions, transverse both to the intra-organizational environment and the inter-organizational environment, is responsible for the non-restriction of the internal control system. Thus, it is applied not only to the intra-organizational control but also to the inter-organizational control, as one can see in figure 3. The intra-organizational control, when dealt with separately in the traditional commercial transactions, is extended in order to include the inter-organizational controls, which were taken in consideration separately in the traditionally transactions.

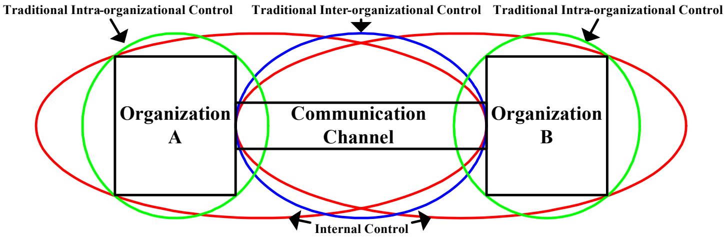
Traditional Intra-organizational Control
Traditional Inter-organizational Control
Traditional Intra-organizational Control
Organization A
Communication Channel
Organization B
Internal Control

Figure 3. The internal control, when in an electronic commerce environment, includes the intra-organizational and inter-organizational control, both existing in a traditional commercial transaction perspective.

Should the organizations think of cleaving to electronic commerce strategies, two main principles of internal control should be taken in consideration: the type of controls in the e-commerce sphere of action and the availability of the mentioned organizations on what regards having a specific framework which will help them in the implementation of an adequate internal control system (Osborne 1999).

The adoption of a coherent and consistent framework that supports the effective implementation of an internal control system, based on the risk associated with the business processes and with the involved information systems, in the e-commerce sphere of action, should take in consideration the need to extend the intra-organizational environment of each of the involved entities to the inter-organizational environment (information and communication channel) that already exists between the above mentioned entities. This will be easily obtained among organizations that have already installed a coherent and consistent internal control system, supported by the same framework or not, with well defined internal control criteria.

4. AUDITING PRACTICES

Despite the fact that, in the last few years, some attention has been given to several e-commerce models, very few of these discussions have been dedicated to the study of internal control systems, which would face the new risks brought along with this new type of e-commerce. Another item that hasn't been subject to much discussion is the proper way to perform auditing in an e-commerce environment (Yu, Yu et al. 2000; Harkness and Green 2004).

The electronic commercial transactions, rendered effective trough the use of the internet as the way for implementation of the necessary information and communication channels, have brought new risks, associated to the business processes and to the information systems that support the above named commercial transactions. These new risks are directly related to the global risk of auditing and, consequently, to its practices. One of the primary aims of the implementation of risk based internal control systems, dealing with the intra-organizational and inter-organizational controls in a holistic fashion, is the global management of auditing risk, according to three of its components: (1) inherent risk; (2) control risk and (3) detection risk:

- **Inherent risk** – the risk of an existing error, material or important when combined with other errors; inherent risks exists, even though an auditing is done, due to the business nature;
- **Control risk** – the risk that there is a material risk, which is not prevented or quickly detected by the internal control system, according to the organization's desire of risk and to the defined risk management criteria;
- **Detection risk** – the risk that the information systems auditor should use inadequate test procedures and could, thus say that there are no existing material errors, when there are.

The global risk of auditing in the sphere of action of electronic transactions that can occur in e-commerce is managed by controlling the involved business processes and the information systems that supports them.

Figure 4 shows what we, in this paper, have considered to be a controlled business process. The controlled business process is obtained by using the technology of software agents. The control process is mainly formed by the software agents that identify possible incongruities when compared to what is real or expected. The software agents are also responsible for the correction of the possible error in real time.

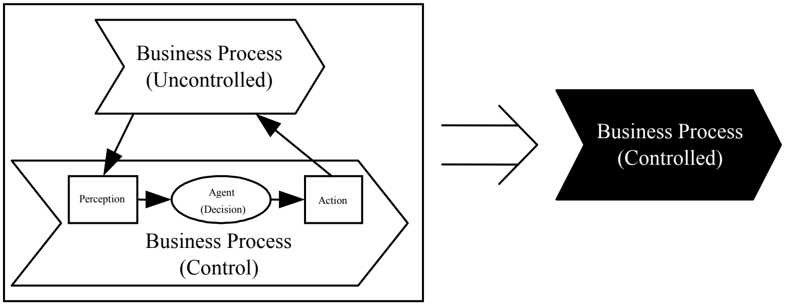

Figure 4. Controlled process, achieved using the software agents' technology.

On an e-commerce environment, the information systems, the intra-organizational business process that support the commercial transactions and the inter-organizational processes and systems that use the internet as a technological infra-structure, to implement information and communication channels of information and communication, are not operated in an independent manner (Pathak 2003). One can verify the coexistence of the business process and the information systems that support them. Besides, the entities involved in the transaction are also common.

In order for the correct management of the auditing global risk, associated to the implementation of e-commerce strategies, the partaking of the auditing function of information systems in every stage of the cycle' development of the processes and systems should be considered, in order for control mechanisms to be installed, based on risk, that prove adequate to each of the types of risk related to the global risk of auditing. An effective internal control system in an e-commerce environment, as above mentioned, should be analysed in an holistic fashion, giving equal importance both to the intra-organizational control mechanisms and to the inter-organizational control mechanisms. One should not forget that, on the e-commerce sphere of action, these two types of control have been joined in a unique internal control system.

Since there is no single entity responsible for the management and exploration of the networks and the respective infra-structures that support the internet, but an highly and varied number of these entities (ANACOM 2004), the implementation of an internal control system that manages the risks associated to the usage of the internet is not common. The implementation of such on internal control system would be much easier if the entities involved in the electronic transaction had themselves implemented an internal control system, supported by a coherent and consistent framework.

By what has been exposed above, we can conclude that, once decisions has been taken, by an organization, to do electronic transactions, it is essential to have a solid business risk management framework.

In this paper we shall use the framework suggested by COSO, named "Enterprise Risk Management Framework", to assure a holistic analysis of the internal control, on what regards e-commerce. One opinion is that this framework for risk management, even though it is not in its complete version yet, which should happen by the middle of September, has proved to be a good framework for the approach of the internal control in a risk management perspective.

5. ENTERPRISE RISK MANAGEMENT

The framework released by the COSO (Committee of Sponsoring Organizations of the Treadway Commission) entitled "Enterprise Risk Management Framework" establishes a sequence of events for the enterprise risk management in control environment: (1) Defining the organizations aims; (2) Risk evaluation (identify it, measure it, prioritize it); (3) Risk Management (control it, avoid it, share it).

The COSO ERM framework 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 COSO ERM Framework defines the enterprise risk management as a process, 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 that constitute it are (COSO 2003):

- **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 likelihood 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 ERM framework can only be seen as truly effective when all of its eight components, above identified, are present and correctly functioning.

6. REAL-TIME E-COMMERCE AUDITING

The electronic commercial transactions real-time auditing should be backed up by a strong theoretical component, which will enable its conceptualization from an epistemological point of view, making it thus easier the design of an adequate organizational and technological architecture. As we have previously mentioned this theoretic component is mainly based on the fusion of intra-organizational controls and inter-organizational controls, supported by a coherent and consistent framework, which will allow one to manage the business risk in a holistic perspective.

The efforts that have been made towards this aim, on the sphere of action of the present information systems auditing procedures, are scattered and the desired effects haven't been accomplished (Mantilla 2001), probably due to its mainly practical component and to the difficulties that arise when one tries to implement control systems in internet supported environments.

In this paper we have chosen an approach to real-time e-commerce auditing, based on the agents software technology. This technology is particularly suitable for the dynamic characteristics of the internet; the best means for inter-organizational transactions; and of the intranets, the best means for the intra-organizational transactions.

6.1 Agent Oriented Approach

Although the energy and mass conservation law "… nothing is created, nothing is lost, every thing is transformed …" has a direct meaning in the commercial transactions between organizations and, consequently, in the business process and in the information systems that support them both intra-organizational and inter-organizational, this has been fully understood, not to mention applied, on the electronic commercial transactions control. If we take this fundamental physics law in consideration and should we leap it over to the electronic commercial transactions, we should consider that any transaction between organizations will always have two components. A "direct action" which shall be the main one to which an "indirect action" will always be related, in order to maintain the harmony of the system in which the commercial trades are performed. The internal control systems should guarantee this harmony, by the implementation of adequate technological resources.

Using agents' software enables the construction of a flexible system, which, despite that, maintains a complex and sophisticated behavior, combining highly integrated modulated components. This approach is particularly suitable for the internal control systems.

This approach to real-time auditing, based on the agents software technology, is easily mistaken with the internal control system behavior (thus happening a change of pattern). The main attention is focused on the software agents, which can be portrayed as internal control components instead of being described as a data collecting tool with consequences in the internal control (Nehmer 2003), as in the use of CAAT (computer assisted audit tools).

In this paper, the control is seen as a resource consumed by the business processes and by the information systems. The control is produced trough a control process, as previously discussed. Each of the eight components of the COSO model "Enterprise Risk Management Framework" can be implemented in a software agents' community.

- **Internal Environment** – the knowledge of the internal environment establishes the basis for all other components of the internal control system, providing the necessary discipline and structure. The software agent responsible for the implementation of this element of the internal control system should continuously evaluate the endogenous and exogenous conditionings that affect the appetite of risk to which the organizations can be under;
- **Objectives Setting** – The knowledge of the aims shall help one to implement software agents which will simulate the restrictions that can be verified within the organizational objectives, divided into four types of aims, the business processes and the information systems;
- **Event Identification** – The identification of events that can threaten the realization of organizational objectives can be implemented trough software agents that allow to verify the effectiveness when in operation;
- **Risk Assessment** – the evaluation of the risk that underlie the business processes themselves, alongside with the level of risk that the organization is willing to support is a factor of major significance in the implementation of control mechanisms through software agents' technology. The activities of the above mentioned software agents, which implement this component of the internal control system, include data collecting its time tendency analysis and the communication of this tendency. Some of the risks that are associated with an e-commerce environment include: fraud; loss of privacy and confidentiality; lack of authentication; repudiation; corruption of data; business interruption and inadequate funding (Pathak 2003);
- **Risk Response** – The risk alignment, related to the risk defined in the component of internal control, is dealt with in the sphere of action of this component. Once the alignment has been established, it can be implemented trough software agents. These will allow its real-time verification and the consequent decisions, should irregularities be found;
- **Control Activities** – the control activities (or mechanisms) can be directly implemented by the software agents, specifically designed to decrease the risk always linked with determined process or through the interaction among agents. Some important categories of control activities are: separation of duties; physical controls; information processing controls and performance reviews (Pathak 2003);
- **Information and Communication** – the information and communication can occur both within the community of software agents but also between that community and the organization management. The agents that implement this component of the internal control system have the special function of communicating with the directors' board, responsible for the maintenance of the internal control system. In the sphere of action of this specific internal control component, we can consider that the risk associated with recording, maintaining and reporting are involved (Pathak 2003);
- **Monitoring** – monitoring is a clearly adjusted to the software agents' technology. Its function consist of permanently monitor the records resulting from the transactions that should happen within the organization and referring to these according to the established patterns of the internal control system.

Any recorded irregularity should become part of an exception file. This component involves assessing the quality of internal controls over time (Pathak 2003).

The control objective is to assure, with some certainty, that every operational aims shall be fulfilled with the minimal associated risk, which shall be managed according to the defined risk desire.

On the other hand, in order for the specific control aims to be achieved, it should be assured that the processes that support them are using adequate control resources. These resources are identified taking in consideration the risk management done according to its identification and to the risk desire of each specific organization.

7. CONCLUSION

The evolution of e-commerce, using a public network like the internet as a technological infra-structure to support the implementation of the information and communication channel, has produced a huge impact on what concerns the implementation of internal control systems and the information systems' auditing practices, when the commercial transactions are done electronically.

In the present paper we suggest that, should an organization decide to implement any electronic commerce model that will implement its information and communication channel trough the internet, it should extend its intra-organizational internal control system to its inter-organizational control. The execution of this enlargement is not common and its feasibility is strongly related to the previous implementation of the intra-organizational control, based on a reliable framework, which will assure the coherence and the stability in the implementation of a risk based internal control system.

The extension of the intra-organizational internal control to the inter-organizational control will allow the implementation of a risk based real-time auditing system, using the software agents' technology. This auditing system shall be involved in the core and support processes of any organization that chose electronic commercial transactions, taking advantages from the markets globalization and the internet ubiquity. As a future work attempt, there is still the need of designing the internal control system architecture that we have, in the present paper suggested.

REFERENCES

ANACOM (2004). O Comércio Electrónico em Portugal: O Quadro Legal e o Negócio. Lisboa, Autoridade Nacional de Comunicações**:** 312.

Andersson, M. and G. Nilsson (1997). Preliminary Study: Business Process Control and Information System Suport. Stockholm, Handelshögskolan I Stockholm**:** 16.

COSO (2003). Enterprise Risk Management Framework. DRAFT**:** 152.

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

Harkness, M. D. and B. P. Green (2004). "E-Commerce's Impact On Audit Practices." Internal Auditing **19**(2): pp. 28-36.

Kornelius, L. (1999). Inter-organisational Infrastructures for Competitive Advantage: Strategic Alignment in Virtual Corporations. Eindhoven, Technische Universiteit Eindhoven**:** 216.

Mantilla, S. A. (2001). Auditoria Financiera Ongoing -Auditoria Contínua-. Bogotá, Pontifícia Universidade Javeriana.

Nehmer, R. (2003). Transaction Agents in E-commerce, A Generalized Framework. Smithfield, Berry College.

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

Osborne, K. (1999). "Controlling and Auditing Electronic Commerce." Datawatch(42): pp. 21-22.

Pathak, J. (2003). "Internal Audit E-Commerce Controls." Internal Auditing.

Plavsic, A., T. Dippel, et al. (1999). "IT Facilitating Fraud." International Review of Law Computers & Technology **13**(2): 193-209.

Powell, D. (2000). "Consuming E-Commerce." Australian CPA **70**(8): pp. 42-43.

Smith, G. E. (1999). Network Auditing: A Control Assessment Approach. New York, John Wiley & Sons, Inc.

Yu, C.-C., H.-C. Yu, et al. (2000). "The Impacts of Electronic Commerce on Auditing Practices: An Auditing Process Model for Evidence Collection and Validation." International Journal of Intelligent Systems in Accounting, Finance and Management **9**(3): pp. 195-216.