Particularities of Audit Planning in E-commerce

Laura-Diana Genete, Faculty of Economics and Business Administration, Iaşi, Romania, glaura@uaic.ro
Alexandru Ţugui, Faculty of Economics and Business Administration, Iaşi, Romania, altug@uaic.ro

Abstract

The purpose of our paper is to catch some of the audit particularities in the e-commerce environment. The technological and economic development of the latest centuries resulted in the significant development of the electronic commerce, and the changes made in the manner of executing transactions had important repercussions on the manner of executing the audit. In this context, auditors must adapt their activity to the general evolution tendency, must be able to understand and evaluate not only the financial information, but also the processing techniques used by the information system of the audited companies. Changes in the manner of executing the audit determined by the use of e-commerce are noticeable early on the mission planning stage.

This paper presents the stages of planning an audit mission, the main changes the auditor must bear in mind in case of companies that use electronic commerce and the manner in which these combine with the audit in the classic environment of transactions.

1. Introduction

The worldwide expansion of Internet use lead to the impressive development of electronic commerce. Currently, it represents a system that includes not only the sale transactions – purchase of goods and services that generate direct revenues, but also those transactions that support revenue getting – such as the generation of the demand for those goods and services, the offering of guarantees and various services to consumers, the facility of communication between business partners. [1]

Thus, the technological evolution and the expansion of the on-line transactions concept resulted in the incorporation within the e-commerce concept of all the commercial activities executed by the employment of the information and communication technologies, such as the Internet, virtual private networks (VPN), automated teller machines (ATMs), electronic fund transfers (EFT), electronic data interchange (EDI), supply chain management (e-SCM) and also customer relationship management (e-CRM). [2]

Therefore, the spectacular evolution of the transactions executed in the electronic environment, both as dimension and complexity, as well as the widespread assimilation of the specific practices by companies from various fields of activity and the incumbency of auditing financial situations lead to an increased interest in the research of the audit particularities in the virtual business environment. We must mention that, although there are various particularities in the execution of an audit mission at companies carrying out electronic commerce activities, the purpose remains the same for all the cases, that of communicating an opinion regarding the financial situations, that is, if they are accomplished, in all their significant aspects, according to an applicable standard of financial reference. [3]

Also, it must be pointed out that the main tasks of auditors, as well as the main stages of the audit, are unchanged, modifications being made especially in the audit execution itself and the information sources submitted for verifications [4]:

- Collection of data about the audited system;
- Collection of data about the business practices of the audited organization;
- Protection of the audited data;
- Analysis of the data reliability and accuracy;
- Analysis of the corresponding business practice use;
- Synthesis of the data obtained from the audit in order to be presented;
- Identification of the situations that need improvement.

Further, we present the main stages of the audit planning and an analysis of the particularities occurring in the case of companies that carry out electronic commerce activities.

2. Audit Planning

Audit planning is the first stage of an audit mission and has the following main purposes: the guarantee that all the segments undergoing audit will be handles attentively, the identification of all potential problems and the facilitation of verifications and reviews, the appropriate determination and assignment of tasks among all team members, the maintenance of the costs of work at a reasonable level and the avoidance of possible conflicts with the customer. At this stage, the auditor must bear in mind at least the following fundamental aspects [5]:

- The general economic conditions and those of the customer's field of activity in particular;
- The understanding of the accounting and internal control system in order to decrease the risk of producing errors, shortages of administration and frauds;
- The audit risk and preliminary materiality;
- The nature, duration and extension of the audit procedures that will be carried into effect;
- The coordination, direction supervision and revision of works;

Other aspects, such as: issues in observing the principle of activity continuity, conditions that require special attention, specific terms of the contract, the type of insurance and the deadline for the issue of the audit report.

The audit planning itself comprises six main stages that have to take into account and cover as area of interest all the previously mentioned aspects [6]:

1. knowledge of the customer and of the business environment;
2. getting information regarding the judicial obligations of the customer;
3. the execution of the preliminary analytical procedures;
4. the determination of materiality and risk evaluation;
5. the understanding of the internal control and the evaluation of the control-related risk.

The information obtained in the first three stages supports the auditor in taking the decision to accept a new customer or to continue the cooperation with an existing one, the fee proposed for the audit services and the decisions the auditor will take regarding the probative elements to be collected, the obtaining of the information that will have to be checked along the mission, the appointment of the employees that will be part of the auditing team, according to the specific nature of the audited company and each one's experience, and the obtaining of a commitment letter. [6]

The last stage of the audit (omitted in the previous enumeration) is the elaboration of the *general audit plan* based on which the auditor will create the *audit programme*. The latter has as a purpose the systematic emphasis of the observance of the procedures stipulated in the International Audit Standards in order to accomplish the mission. The audit plan and programme can be reviewed and modified during the execution of works, the auditor being forced to record all the important changes, as well as the reason of their execution, in the mission file.

The companies' use of the virtual environment for the execution of goods and services transactions results in significant changes in the audit planning activity, especially when it has a significant effect on the entity's business. In this case, the auditors need to consider the required information technology and Internet business knowledge which involves [7]:

- understanding the impact of the entity's e-commerce strategy and activities, the technology used, and the risks involved on the financial statements;
- determining the nature and the extent of audit procedures and the method used to evaluate audit evidence;
- considering the extend of e-commerce activities and their potential risks on the entity's ability to continue as a going concern.

The above-mentioned aspects must be analysed by auditors in order to identify the way in which they influence the activity of the audited company and the audit-specific works, both in the work planning stage, and later, during the mission.

2.1 Knowledge of the customer and of the business environment

The first stage of the audit works planning resides in knowing the customer, of the general economic conditions and those of the field of activity, knowledge which is essential for the estimation of the audit works and absolutely necessary for at least two reasons: (1) there are economy branches that have unique accounting circumstances that the auditor must know and understand, (2) the auditor can identify certain risks specific to the branch that might influence the audit risk level. In the case of the companies that use the e-commerce, the auditor must obtain enough information so as to identify and understand the events and transactions and the practices specific to them and that can significantly influence the financial situations. They include the entity's [7]:

- business activities and industry;
- e-commerce strategy;
- extent and risks of e-commerce activities;
- outsourcing arrangements.

The information sources the auditor can use in order to know the company's field of activity are diversified and include: discussions with auditors from the previous years and with those involved in similar missions, meetings with the company's staff, direct analysis of the customer's activity, manuals of the specialized bodies, magazines with technical character in the field etc. Modern information and communication technologies offer companies, both to the ones that perform activities in a classical manner, and also to those that use the virtual environment to develop transactions, further information sources regarding the field of activity which the audited company works in, as well as the customer's activity itself [8]:

- *intelligent agents* – trained to navigate on the Internet and gather information about a certain company or field of activity;
- *knowledge management systems* – developed and used by the accounting companies about the customers' branches of activity and about the best practices in the field of interest;
- *on-line searches* – materialized either in information offered by companies specialized in such activities, or in using the search engines directly by the auditors to obtain information or by using the sections dedicated exclusively to financial problems or to discussion forums where one can get opinions about various companies or fields of activity;
- *the website of the audited company* – it can be an important source of information for the understanding of the company's strategy and the identification of products and services offered to customers, inclusively under the aspect of technical and financial data accuracy;
- *economic statistics* – statistic yearbooks offer important information on the fields of activity at a regional, national and international level, and

some of them are available online. The auditor can compare the results of the customer with other economic data in the field and can have an image of that company's position on the market;
- *analysis reports* – they concern the information provided by the companies that market actions about the economic organization from various fields, their strategies, management quality and success probability, that can be used by the auditor for better knowing the customer and the business environment.

2.2 Getting information regarding the judicial obligations of the customer

The second stage in audit planning is to get information regarding the judicial obligations of the customer. The execution of this stage requires the analysis, by the auditor, of at least the following documents [6]: the founding status and the internal regulations, the records of the board of directors meetings and those of the shareholders, as well as the enterprise's contracts. These documents are used both to identify the activities the company develops and/or is entitled to develop, the commitments the company assumed, as well as to check the existence (or absence) of the approvals needed for every commitment or signed contract. The information obtained at this stage is important in order to estimate the extension of the mission works and to identify the inherent risks.
In case of using the electronic commerce, special attention must be paid to contracts in which all the operations take place in the virtual environment, from contacting the customers, by mail or electronic forms, to the moment of signing the contracts using the digital signature. In this case, the auditor must follow and check the data veracity, exhaustiveness and accuracy in order to detect possible frauds, which are often more difficult to identify due to the virtualisation of operations. In this case, a significant role is held by the communication services provider that, without being directly involved in transactions, offers the technical support for the transmission of information from the company to the customer and the other way round. In this situation, auditors can request the obtaining of the procedure manuals and the provider's policies, as well as the logs of the transactions, in order to better understand the international flows among the customers – audited company – suppliers. The applications used for electronic transactions must use the latest crypting technologies for electronic signatures and certificates and for securing the servers in order to assure the auditor that the information exchange is made in conditions of maximum security. [9] All these independent verifications are used to guarantee that all the security controls are adequate and they protect the organization, providers, partners and customers from possible security gaps and they must always be updated to the latest changes that take place in the information and communication technology.

2.3 The execution of the preliminary analytical procedures

The execution of preliminary analytical procedures is the third stage of an audit mission planning, having as a purpose the establishment of the nature of works, of the duration, and the level of particularization of works. In many situations, at this stage, the auditor considers as sufficient the analysis of the last few years' main economic indicators of the customer comparing to the branch of activity. Of all these indicators, the most important are the liquidity, solvability, the degree of indebtedness and the capacity to cope with payment obligations, the indicators of exploitation and of the results.

2.4 Materiality and audit risk evaluation

Materiality and audit risk evaluation is the fourth stage in the work planning activity and at the same time the most complex, having a decisive role in the future development of the mission. Both the proportion of the future verifications and their accuracy, as well as the concordance with the reality of the auditor's final opinion, depend on the efficiency and correctness of this stage.
Materiality is defined in the International Accounting Standards Board's "Framework for the Preparation and Presentation of Financial Statements" as follows: *information is material if its omission or misstatement could influence the economic decisions of users taken on the basis of the financial statements. Materiality depends on the size of the item or error judged in the particular circumstances of its omission or misstatement. Thus, materiality provides a materiality or cut-off point rather than being a primary qualitative characteristic which information must have if it is to be useful*. [10]
The establishment of materiality is difficult because it concerns, at the same time, *quantitative* and *qualitative* aspects. This difficulty is increased by the fact that, according to the definition given by the Financial Accounting Standards Board, the auditors must know who the users of the financial situations are and what elements constitute their basis.
The audit norms suggest using one of the following indicators in order to establish the materiality: 1%-2% of the total actives, 0.5%-1% of the turnover or 5%-10% of the profit before taxation. Most often the auditors refer to the *profit* of the audited company, as it reflects the results in the best manner. If there are significant differences between the profit values from one year to another, *the average profit on the last three years* can be used as reference. In the case of companies that have losses, the materiality can be determined based on the profit from the years when they performed their activity in normal conditions. The materiality level thus determined will have a

global materiality and it must be allotted at the level of the accounts and individual transactions by establishing some *individual materiality*.

As regards the quantitative evaluation of the materiality, it can have important repercussions on the company's activity and results if it exceeds a certain level. [11]. An example of qualitative error is represented by the deviations involving frauds, considered to be more important than the unintentional errors of identical monetary values, because fraud is an indicator of the lack of honesty from managers or other employees involved in it.

An important constituent of the audit planning is represented by the risk evaluation, similar, to a certain extent, to the one used in the classic environment audit. According to specialists' opinion, there are four risk areas that can be felt at the audit level [8]:

1. *the enterprise risk* – those risks that affect operations and possible results of the company's activity;
2. *commitment risks* – the risks resulted from the association between the auditor and a certain customer: losing the reputation, the customer's inability to pay the auditor, financial losses resulted from an incorrect management or that limit/restrict the auditor's mission;
3. *the risk associated to financial situations* – risks related directly to transactions recording and the representation of financial data in the company's situations;
4. *audit risk* – the risk of expressing an opinion without constraint due to the omission of some errors by the auditor .

Another classification divides risks according to the company's possibility to influence them and respond to them [12]:

- *controllable risks* – risks that exist within the processes of an organization and that are wholly in the hands of the organization to mitigate;
- *uncontrollable risks* – risks that arise externally to the organization and that cannot be directly controlled or influenced but that nevertheless call for a risk position to be taken by the organization;
- *influenceable risks* – risks that arise externally to the organization but that can be influenced by the organization.

The informational environment involves new risk categories associated to its components, out of which the following are the most significant [10]:

- *operations* – sabotage, natural disasters, viruses, threatenings that affect the operating ability;
- *programs* – fraud programming, incomplete or incorrect data processing, fraud data processing;
- *files* – unauthorised access in order to destroy or manipulate data from the reports, analyses or business development, the contamination by adding unauthorized data;
- *communication* – interception, modification, deletion or replacement of data with fraud data; ports allowing the access of hackers, denial-of-service attacks, unauthorised access to data and programmes.

In order to evaluate and establish the audit risk, the International Audit Standards stipulate the analysis, by the auditor, in the mission planning stage, of the following main risk categories [10]:

- *inherent risk* - the susceptibility of an assertion to a misstatement, that could be material, individually or when aggregated with other misstatements assuming that there were no related internal controls;
- *control risk* - the risk that a misstatement that could occur in an assertion and that could be material, individually or when aggregated with other misstatements, will not be prevented or detected and corrected on a timely basis by the entity's internal control.
- *detection risk* - the risk that the auditor's procedures will not detect a misstatement that exists in an assertion that could be material, individually or when aggregated with other misstatements.

Audit risk is obtained as a product of the three above-mentioned components:

$$RA = IR \times CR \times DR$$

In the case of companies that have electronic commerce activities, besides the risks specific to the classic environment, there can occur other risks, having a direct or indirect impact on the mission, amplified sometimes by the transfer and electronic archiving of data. For this reason, the International Audit Standards, by means of the ISAP 1013 (Electronic commerce – the effect on the financial situations audit) mentions the following additional risks the auditor must bear in mind when carrying out the mission [13]:

- loss of transaction integrity resulting in loss of audit trail;
- security risks such as virus attacks or e-frauds;
- improper accounting policies relating to, for example, web site development expenditure, recognition of revenue relating to Internet sales, and cut-off;
- non-compliance with taxation and other regulatory matters such as privacy issues and legal protection requirements across international boundaries;
- failure to ensure contracts evidenced only by electronic means are binding;
- overreliance on e-commerce when placing significant business systems or transactions on the Internet;
- systems and infrastructure failures or breakdowns.

The same settlements stipulate the following categories of measures in order to prevent the risks from occurring:

- verification of the customers' and suppliers' integrity;
- assurance of the transaction integrity;
- obtaining the permission for the contract terms, including the delivery agreement, lending conditions and the way of solving litigations that

can refer to the pursuance of transactions and procedures in order to guarantee that one of the parties will not subsequently deny certain specified terms of the agreement;
- obtaining payments from, or assuring lending facilities for customers;
- establishment of protocols for the assurance of confidentiality and the protection of information.

Comparing with the classic environment for performing transactions, the risks associated to electronic commerce are increased due to the use of information and communication technologies.

The analysis of risks associated to audit in the case of organizations that have electronic commerce activities involves both risks similar to the classic information systems, and also specific risks. In the last category we can include [8]:
- System security and the protection against malicious intrusions or the access of people from outside;
- Integrity or exhaustiveness of the processing;
- Integrity of data communication;
- trading partner agreements;
- interdependencies among systems;
- "no paper engagement systems" joined with the "soft control".

The above-mentioned risks have a general character, being valid for all the companies that use electronic transactions. Except for these, there can occur customer-specific risks that the auditor must identify and evaluate.

Obviously, further risks require additional controls in order to prevent them from happening.

2.4 The understanding of the internal control and the evaluation of the control-related risk.

The internal control system is made of the assembly of procedures and policies adopted by the leadership that attend the fulfilment of the managerial objectives regarding the assurance of a systematic and efficient leadership of activities, including the adhesion to managerial policies, the prevention and detection of fraud and errors, accuracy and exhaustiveness of the accounting records, the preparation in due time of the credible financial recordings. [6] Internal controls may have a significant importance in preventing or decrease of e-commerce-determined risks. Thus, according to ISA 400 standard, "Evaluation of risk and internal control", the auditor will analyse the control environment and the control procedures applied by the entity to its electronic commerce activities, as long as these are relevant for the assertions of the financial situations. The following aspects of internal control are considered to be extremely important when the virtual environment is used for economic transactions:

1. *security* considered to be accomplished when the regulations for the authorisation, authentification, confidentiality, integrity, non-repudiation and availability of this information exist and are observed. The most important measures that need to be adopted in order to assure the security of transactions and of the information are the following [8]:
   - Firewall – to intercept the unwanted traffic and, at the same time, to protect the Web server and the back-office server both from the unwanted traffic and from the one intended to destroy the website;
   - Crypting – it transforms the data in a format that cannot be read if it is intercepted by unauthorised users;
   - Monitoring reports – to guarantee that there are no unusual accesses or unusual business types;
   - Electronic transmission protocols – that identify partial losses or data missing from transactions; received messages must be reconciled with the messages sent by the partner;
   - Denial-of-service software to identify the attacks and to stop the message flows directly from the source of attack;
   - Integrated systems, such as the ERP's – that work with transactions made in the electronic environment in order to increase the processing efficiency and the production;
   - Websites security – it guarantees that unauthorised persons or from outside the company cannot modify the site's structure and content;
   - System security and backups – the greatest change of the web-based systems is the 24/7 capability and, for this reason, the designers must guarantee continuous availability, even if a par of the system is down. The system must be capable of redirecting the traffic towards another server in case one of them is down.
2. *integrity of transactions* regards exhaustiveness, accuracy and authorisation of the information provided for being recorded and processed in the financial recordings of the entities. This component requires verifications concerning the following aspects at least [13]:
   - validation of entries;
   - prevention of duplicates or possible transaction omissions;
   - the guarantee that the terms of transactions were accepted before the processing of orders, including the delivery and lending conditions;
   - the differentiation between the site's visitors and buyers;
   - the guarantee that a participant in the transaction cannot deny the transaction after the conditions have been accepted;
   - exact specification of the terms of transactions and the guarantee that the involved parties accept them;

- prevention against incomplete processing by guaranteeing the compulsoriness of going through and registering of all the information specific to each stage or the rejection of the registrations if at least one stage was not complete;
- corresponding distribution of all the transaction details in all the systems belonging to the network;
- proper keeping of registrations and backups and their securization.

3. *process alignment* concerns the manner in which systems based on information technologies are integrated in the information system of the company in order to work as a whole. In the e-commerce environment it is fundamental that the online transactions be taken over and processed correctly in the entity's internal system and, since in many case the organization websites are not integrated in the internal entity's system, increased attention is needed so that all the operations be taken over and processed accordingly. This aspect may significantly influence the following aspects [13]:
   - exhaustiveness and accuracy of the transaction processing and data storage;
   - recognition of revenue from sale, acquisitions and other types of transactions;
   - identification and registration of litigious transactions.
4. the maintenance of the control procedures in the continuously changing environment, both from an economic and technical point of view, specific to electronic commerce;
5. the assurance of access to relevant recordings, necessary for meeting the information needs within the organization, as well as the audit execution in optimum conditions.

After the internal control analysis and understanding, the auditor must estimate the control risk, either by using qualitative (large, medium, small) or quantitative (numerical) estimations. Usually, the estimation of the control risk is performed at the level of every audit objective related to operations and for every important operation type. The control risk estimated at this stage, together with the inherent risk and the accepted audit risk, will be used to determine the risk of non-detecting and, furthermore, to establish the patterns' size.

3. Conclusion

Our paper intended to identify the main changes that take place when planning an audit mission in the case of electronic commerce use. From what has been presented above, we can infer a few conclusions:

- The expansion of electronic commerce use has a strong impact on the audit mission early on the work planning stage;
- The main principles of an audit mission for companies using electronic commerce are identical with the ones of companies that perform only classic transactions, but there are significant changes at the level of the methods used to accomplish the mission;
- Audit according to the classic methods can often be insufficient in the virtual environment and, thus, auditors must adapt their practices according to the way activities are performed and often they must improve their knowledge in order to meet the requirements imposed by the use of information and communication technologies;
- Electronic commerce transactions substantially increase the volume of work in the audit planning stage and they bring numerous particularities that have to be analyzed and understood by the auditor;
- Continuous audit could be an efficient solution for the audit, but the level of evolution it has currently reached is insufficient to be considered an efficient alternative of audit made by the human specialist.

Mention must be made that the study catches only a part of the changes determined in the work planning stage by the movement from the classic manner of doing business to the virtual environment, with the purpose to set the bases of an e-commerce audit model.

6. References

[1] Kosiur, D., *Understanding Electronic Commerce (How OnlineTransaction Can Grow Your Business),* Microsoft Press, Redmond, Washington, 1997.

[2] Pathak, J., *Information Technology Auditing. An Evolving Agenda*, Springer-Verlag, Berlin, 2005.

[3] International Federation of Accountants, ISA 200 - Overall Objective of the Independent Auditor, and the Conduct of an Audit in Accordance with International Standards on Auditing.

[4] Carter, J., *Developing e-Commerce Systems*, Prentice-Hall, Inc., 2002, New Jersey.

[5] Dobroţeanu, L., *Audit – Concepte si Practici*, Ed. Economică, 2002.

[6] Arens, A., Loebbecke, J., *Audit. O abordare integrată*, Editura Arc, 2003.

[7] Cosserat, G., W., *Modern Auditing*, 2nd Edition, John Wiley & Sons, Ltd., England, 2005.

[8] Rittenberg, L., Schwieger, B., Johnstone, K., *Auditing. A Business Risk Approach*, 6th Edition, Thomson South-Western, Manson, USA.

[9] Busta, B., "Encryption in Theory & Practice", in *The CPA Journal*, No. 72/11. November 2002.

[10] International Federation of Accountants, *Handbook of International Auditing, Assurance, and Ethics Pronouncements*, Retrieved April 15 2008, http://www.ifac.org/Store/Category.tmpl?Category=Auditing%2C%20Assurance%20%26%20Related%20Services.

[11] Ricchiute, N., D., *Auditing*, 3rd Edition, South-Western Publishing Co., 1992.

[12] Casarino, E. R., *Auditor's Guide to Information Systems Auditing*, John Wiley & Sons, Inc., New Jersey, Canada, 2007.

[13] IAPC (2002) IAPS 1013 - Electronic Commerce: Effect on the Audit of Financial Statements, Retrieved February 10, 2008, http://www.paab.co.za/documents/doc_00301.pdf.