Changing Methodologies in Financial Audit and Their Impact on Information Systems Audit

Daniel VÎLSĂNOIU, Mihaela ŞERBAN
Doctoral School – Accounting and Management Information Systems
Academy of Economic Studies, Bucharest, Romania
dan.vilsanoiu@gmail.com, mihaela.serban@gmail.com

This paper tries to provide a better understanding of the relation between financial audit and information systems audit and to assess the influence the change in financial audit methodologies had on IS audit. We concluded that the COSO Internal Control – Integrated Framework was the starting point for fundamental changes in both financial and IS audit and that the Sarbanes-Oxley Act should be viewed as an enabler rather than an enforcer in establishing strong governance models. Finally, our research suggests that there is a direct causality effect between the employment of BRA (business risk audit) methodologies and the growing importance of IS audit.

Keywords: *Financial Audit Methodologies, Business Risk Audit, Information Systems Audit, Internal Controls Framework*

1 Introduction

The objective of this article is to provide a better understanding of the relation between financial audit and information systems audit and to assess the influence the change in financial audit methodologies had on IS audit.

In order to achieve our objective, we reviewed existing research from both academics and professionals regarding financial and information systems audit methodologies. We also obtained and reviewed materials from leading professional organizations in financial and information systems auditing, such as the International Auditing and Assurance Standards Board (IAASB), the American Institute of Certified Public Accountants (AICPA), the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI).

According to [1], the purpose of a financial audit is to enhance the degree of confidence of intended users in the financial statements. This is achieved by the expression of an opinion by the auditor on whether the financial statements are prepared, in all material respects, in accordance with an applicable financial reporting framework.

In [2], the information systems audit is defined as the process of collecting and evaluating evidence in order to determine whether the information systems and related resources adequately safeguard assets, mentain data and system integrity and availability, provide relevant and reliable information, achieve organizational goals effectively, consume resources efficiently, and have, in effect, internal controls that provide reasonable assurance that business, operational and control objectives will be met and that undesired events will be prevented or detected and corrected in a timely manner.

We begin by noticing that starting from the mid 1990s, a change in financial audit methodologies occurred. This change was characterized by shifting the focus of auditors from financial statement risk to business risk and by the employment of new types of audit procedures such as testing supervisory controls and high precision analytical work.

We continue by summarizing the features of the "old" and the "new" audit methodologies and with an analysis of what caused this shift and what are the main advantages and disadvantages of the new audit methodology.

In the 3rd chapter we focus on how laws and regulations that were initially addressed to financial auditors influenced information systems auditing and in the 4th chapter we link the evolution of the IS audit profession with the adoption of new financial audit methodologies, which allowed the rapid growth of revenues generated from non-audit services for large audit firms.

We finish by presenting our conclusions and by proposing some possible areas of research.

2 Transaction cycle vs. Business process audit methodologies

After reviewing prior research about audit methodologies and technological changes in financial audit practices, it became apparent to us that all authors agree that in the 1990s there has been

a shift in methodologies applied by financial audit professionals. While there are differences in terminologies between authors and there is some debate about when the change has occurred and what caused it, all of them recognize the existence of an old and a new audit paradigm.
All citied papers state the old audit methodologies are transaction cycle oriented and the new methodologies are business process oriented. According to [3], the change in the audit approach was achieved by:

- focusing the audit to business risk rather than financial statement risk
- changing the nature of audit work from substantive procedures (i.e. large volume tests of details) to the testing of supervisory controls, supported by high precision analytical work

The main differences between these financial audit paradigms are summarized in Table 1.

Table 1. Comparison of traditional and new business risk paradigms [4]

Transaction cycle oriented audit approach	**Business process oriented audit approach**
Risk assessment occurs periodically	Risk assessment is a continuous process
Accounting, Treasury and Internal Audit responsible for identifying risks and managing controls	Business risk identification and control management are the responsibility of all members of the organization
Fragmentation – every function behaves independently	Concentration – Business risk assessment and control are focused and coordinated with senior level oversight
Control is focused on financial risk avoidance	Control is focused in the avoidance of unacceptable business risk, followed closely by management of other unavoidable business risks to reduce them to an acceptable level
Business risk controls policies, if established, generally do not have the full support of upper management or are inadequately communicated throughout the company	A formal business risk controls policy is approved by management and board and communicated throughout the company
Inspect and detect business risk, then react to the source	Anticipate and prevent business risk and monitor business risk controls continuously
Ineffective people are the primary source of business risk	Ineffective processes are the primary source of business risk

2.1 Transaction cycle oriented audit

Transaction cycle oriented methodologies or TFAs (transaction-focused approaches), as they are referred to in [5], are highly structured top-down approaches of the audit process which constrain the range of actions available to individual auditors in specific circumstances and are characterized by rigid decision making processes [6].
These methodologies do not require the auditor to gain a deep understanding of the auditee's business strategy (and resulting business risk) as this information is used only in the pre-audit or planning activities and no implications of the business risks are considered when determining audit risk [7]. At best, auditors are required to concentrate their attention to account-level factors before considering the influence of business risk factors. [5]
The main objective of transaction cycle oriented audit methodologies is to reduce the risk of auditors making judgmental errors and provide for a rationale for issuing audit opinions which is strong enough to withstand reviews from peer auditors or regulators. In order to achieve this objective, a range of tools and techniques was developed or refined so that it would meet the required level of assurance for issuing audit opinions (e.g. statistical sampling, risk based testing, analytical procedures, decision aids and going concern evaluation) [6].

2.2 Business process oriented audit

In [8] – paragraph 4-b, business risk is defined as the risk resulting from significant conditions, events, circumstances, actions or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies.
The idea that anything that increased business risk also increased audit risk [9] first emerged in the mid 1990s and eventually led to a shift in audit methodologies. Arguing that "anything that had the potential to increase the risk that an organization would not meet its objectives is a source of increased audit risk" or simply "busi-

ness risk drives audit risk" [6], members of the academic and audit community developed new, business process oriented, audit methodologies that were commonly referred to as BRA (Business Risk Auditing) or Strategic Systems Auditing (SSA) [10].

Some authors claim that broadening perceptions in risk such as enunciated in the Committee of Sponsoring Organizations for the Treadway Commission (COSO) report, Internal Control – Integrated Framework (1992) paved the way for the new BRA methodologies emergence. [6]

The standard scenario for using these methodologies is [4]:

1. Modeling business risk processes of the client company.
2. Mapping the client's strategy to the related business risks.
3. Using the knowledge about the client's business risks as the basis for determining audit risks.
4. Perform audit tests according to the identified audit risks.

A key benefit that led to the development and use of BRA methodologies by financial auditors was the greater added value that could be provided to the client. A better understanding of the client's business strategy would presumably allow auditors not only to better evaluate audit risks but also to identify other potential risks or areas of improvement for the client. It was claimed that by employing BRA methodologies, auditors could comment on business risks and also on their impact over financial statements [4].

In other words, by performing a comprehensive review of all business risks during the process of identifying audit risks, a so called "knowledge spillover" [4] from the audit would be generated. This would result in extra feedback provided to the client which would get more information for his money.

In order to better evaluate risks, auditors analyze variations in metrics that provide key performance indicators (KPIs) for business processes and then integrate their knowledge of business risks with evidence about changes in accounting metrics [5].

2.3 Causes of the change

The most commonly cited causes for the shift in audit methodologies are:

- Large audit firms (formally known as the Big8, Big6, Big5 and nowadays Big4) enforced BRA methodologies in their attempt to increase their revenues by widening their area of expertise from audit to consulting services. [6], [4]
- Poor regulation of audit markets allowed large audit firms to pursue revenue growth by providing consulting services [6]
- Changes in technology increased the likelihood of financial misstatements so auditors looked for methods of incorporating business risk more directly in their audit risk assessment in order to respond to their clients need for assurance. [4] [5]
- The growth in internal audit services within client companies led to pressures on auditors to reduce fees on the claim that part of the assurance was provided by the internal audit function [6]
- Although cost cutting has always been an objective of the audit firms, using BRA methodologies allowed auditors to achieve this goal by using less resource consuming substantive procedures [4] [7]

2.4 Discussion: pros and cons of the business process oriented audit

We noticed that although authors agree on the shift in audit methodologies, there is a debate about how beneficial was the change for the audit profession.

Supporters of the BRA methodologies claim that auditors who use them are more likely to integrate evidence about business risk directly into their planning judgments about the risk of material misstatement [5] [11], because of the way information about business risks and their impact on audit risk is structured in the BRA approach.

In [1] – paragraph 13-n, the risk of material misstatement (RMM) is defined as the risk that the financial statements are materially misstated prior to audit. This consists of two components, described as follows:

- Inherent risk – The susceptibility of an assertion about a class of transaction, account balance or disclosure to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls.
- Control risk – The risk that a misstatement that could occur in an assertion about a class of transaction, account balance or disclosure and that could be material, either 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.

Furthermore, BRA methodologies are analyzed and recommended as a response to changes in the

audit environment and to the stakeholder's growing demand for protection against financial statements fraud.
According to [7], auditors who use the SSA approach must build their assurance that management's financial statements present a true and fair view of the audited entity by having a clear understanding of the entity's business strategies, conditions, processes, and economic actions/events, as well as past, current, and likely future business relationships with other entities.
Critics of BRA methodologies claimed that auditors (especially large audit firms) used them to open the possibility for more lucrative non-audit (consulting) services that could be provided to clients following a complete business risk evaluation [6].
They also claimed that these methodologies failed to prevent or even warn the public about major financial collapses of companies (e.g.. Enron) or on the financial crisis which began in 2007. In [12], it was noted that many financial institutions which sought state support were given unqualified audit opinions by large audit firms (mainly Big4 companies) shortly before their collapse. Questions were raised about auditor's independence (all of the auditors collected large amounts of audit and non-audit fees from their clients) and quality of work (the BRA methodology was being put under scrutiny).
Another shortcoming of the BRA methodologies is that even experienced auditors find it difficult to link business risks and related controls with financial statement amounts. While in theory it was generally accepted that business risk is related to audit risk, practitioners were uncomfortable with this inference in auditing (giving an audit opinion on the financial statements based on indirect evidence drawn from analysis concerning business risks and the operation of high level controls) [3] [9].
This is why regulatory initiatives that followed from the aftermath of Enron, tried to bridge this gap by reconsidering business risk audit methods in the form of combining the best from transaction focused audits with the best from business risk auditing [6]. This goal was achieved by audit practitioners by performing more substantive audit procedures [3].
The debate about BRA methodologies is likely to continue in the following years, with some authors calling for more research on how to organize business process information for auditor use in audit risk assessment [13] and for more research into the efficacy of the risk-based audit approach that is now embodied in professional standards [5].

3 The impact of financial audit regulations on information systems auditing

In this chapter we consider the way laws and regulations that were initially addressed to financial auditors influenced information systems auditing. We focused on the Sarbanes-Oxley Act of 2002 which requires organizations to select and implement a suitable internal control framework and on the COSO Internal Control - Integrated Framework which has become the most commonly adopted framework by public companies seeking to comply with the new regulations [2].

3.1 The COSO Internal Control – Integrated Framework

In 1992 COSO published what now is referred to as the COSO Model of Internal Control (Figure 1) and when AICPA adopted the COSO Model as Statement on Auditing Standard (SAS) No. 78, "Consideration of Internal Control in a Financial Statement Audit" it became a part of the technical literature for financial auditors. [14]
Although audit professionals were very well familiarized with the concept of risk, the COSO Model of Internal Control caused the challenging of conventional (transaction cycle oriented) audit approaches inside the audit profession and eventually led to the development of "business risk audit" methodologies [6].
Also, the COSO model emphasized the concepts of risk and risk management to audit professionals, by identifying new dimensions of internal controls that were relevant to the conduct of an audit [6]. There were five dimensions that were depicted in the COSO "internal control cube" (figure 1):

- control environment (the circumstances of the client)
- risk assessment (the ability to identify threats)
- control activities (the actions taken to intervene)
- monitoring (the maintenance of controls),
- information and communication (the ability to coordinate all dimensions)

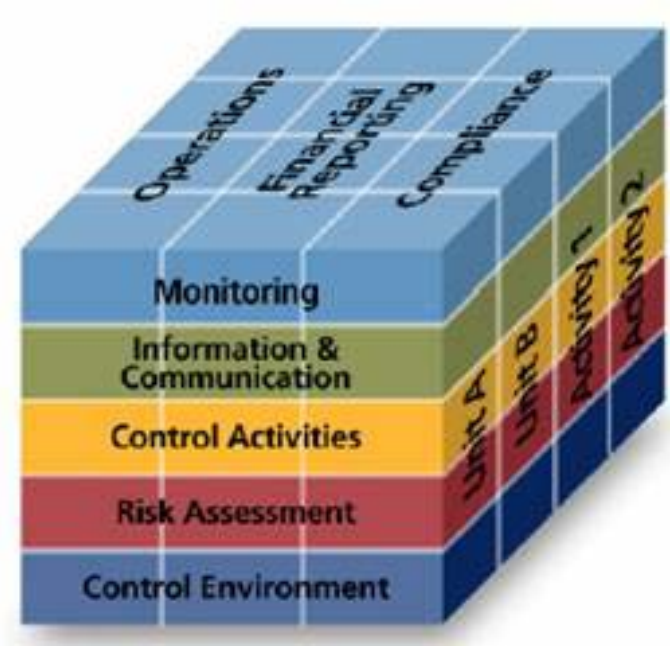

Fig. 1. The COSO internal control cube [15]

Because most of the internal controls that were relevant to financial audit were relying on IT, an increasing demands that IS auditors provide assurance regarding the IT based controls emerged. This is why

The internal controls dimensions, which are used by financial and IS auditors in performing their work, can be detailed as follows [14]:

The control environment element is a view of internal controls from the entity's perspective. Some of the ways the risks associated with the control environment can be evaluated include:

- Communication and enforcement of integrity and ethical values;
- Commitment to competence;
- Participation of those charged with governance;
- Management's philosophy and style;
- Organizational structure;
- Assignment of authority and responsibility;
- Human resource policies and practices;
- Industry factors.

The risk assessment aspect of COSO, refers to the entity's ability to properly assess risks and, for major ("significant") risks, mitigate them to an acceptable level using controls. Areas where controls and/or procedures should be developed to enhance the entity's system of controls include:

- Changes in operating environment;
- New personnel;
- New or revamped information systems;
- Rapid growth;
- New information technology employed;
- New business models, products or activities;
- Corporate restructurings;
- Expanded foreign operations;
- New accounting pronouncements.

Controls are evaluated at three levels: design effectiveness, implementation and operational effectiveness and some of the various ways to evaluate control activities include:

- General controls:
  - Policies and procedures related to the service/product provided;
  - Controls over support (especially computer systems and operations, networks, etc.);
  - Changes to systems associated with core business processes;
  - Environmental security;
  - Application development, maintenance and documentation;
  - Information security;
  - Disaster recovery/business recovery;
- Application controls:
  - Tests of control;
  - Controls embedded in various applications to satisfy management's policies and procedures for carrying out business processes.
- Physical controls:
  - Authorization of service instance;
  - Segregation of duties (if applicable, IT personnel too);
  - Supervision;
  - Audit trails;
  - Access controls to systems and data;
  - Independent verification (performance re-

ports, independent reviews, audits, error logs, etc.).

The information and communication element of the COSO model requires that financial reporting information should have reliability and should be communicated in a timely and accurate manner to managers and decision makers.

Information and communication risks can be evaluated include:

- Systems to support the identification, capture and exchange of information in a form and time frame that enable personnel to carry out their responsibilities;
- Financial reporting information;
- Internal control information;
- Internal communication;
- External communication.

Monitoring refers to the entity's ability to monitor the effectiveness of controls as they operate daily, individually and in cooperation with other controls. Some of the various ways in which controls over monitoring of control effectiveness can be evaluated regarding the risks associated with those activities include:

- Ongoing and separate evaluations on internal controls over financial reporting;
- Identifying and reporting deficiencies;
- Assessing the quality of internal control performance over time;
- Putting procedures in place to modify the control system as needed (add, change, delete);
- Ensuring effective management review of control system status;
- Checking for the absence of monitoring systems, which tends to allow people to reduce vigilance on controls;
- Utilizing relevant external information or independent monitors;
- Analyzing control objectives and their related control activities;
- Reviewing changes to controls since the date of the last report or within the last 12 months.

3.2 The Sarbanes-Oxley Act

Another regulation that had a major impact on information systems audit was US Sarbanes-Oxley Act of 2002 (or SOX). Section 404 of Sarbanes-Oxley requires management to do an evaluation of internal controls and financial auditors to opine on that evaluation. In addition, the Act created the Public Company Accounting Oversight Board (PCAOB) as an agency to provide oversight of financial reporting for publicly traded companies and report to the US Securities and Exchange Commission (SEC) [16].

The act was aimed primarily at public companies boards, management and audit firms by prohibiting registered public accounting firms from performing certain non-audit services for a public company client for whom it performs financial statement audits. Such prohibited non-audit services include internal audit outsourcing services and financial information system design and implementation [4].

Sarbanes-Oxley experts agreed that IT control was a specific area likely to produce significant deficiencies by many companies. As the majority of internal controls are embedded in automated systems, IS auditors have become a vital part of complying with the standards, guidelines and regulations [17].

This is why IT professional organizations, such as the IT Governance Institute (ITGI), tried to standardize a set of objective and responsibilities for IT departments of audited companies in order to comply to the Sarbanes-Oxley Act.

The following section provides a compliance road map that is tailored to the specific objectives and responsibilities of IT departments [18]:

1. Plan and scope IT controls:
   - Assign Accountability and Responsibility;
   - Inventory Relevant Applications and Related Subsystems;
   - Review Financial Process Documentation and Identify Application Controls;
   - Develop a Preliminary Project Plan and Obtain Approval;
   - Determine Responsibility for Application Controls;
   - Consider Multilocation Issues;
   - Consider Whether Applications Can Be Eliminated From Scope;
   - Identify Dependencies on Third-party Service Organizations (Outsourcing).
2. Assess IT risk:
   - Assess the Inherent Risk of Applications and Related Subsystems;
   - Refine Scope and Update the Project Plan.
3. Document controls
   - Identify IT Entity-level Controls;
   - Identify Application Controls;
   - Identify IT General Controls;
   - Identify Which Controls Are Relevant Controls;
   - Consider IT-based Antifraud Controls;
   - Control Documentation.
4. Evaluate control design and operating effectiveness
   - Evaluate Control Design;
   - Evaluate Operational Effectiveness;

- Consider the Nature of Evidence Required;
- Consider the Timing of Control Testing;
- Roll-forward Testing.

5. Prioritize and remediate deficiencies
   - Consider Guidance From the SEC and PCAOB;
   - Identify and Assess IT General Control Deficiencies;
   - Consider the Aggregate Effect of Deficiencies;
   - Remediate Control Deficiencies.
6. Build sustainability
   - Rationalize Controls;
   - Automate Controls;
   - Perform Application Benchmarking.

In [18], ITGI recommends that the work performed to meet the requirements of the Sarbanes-Oxley Act should not be regarded as a compliance process, but rather as an opportunity to establish strong governance models designed to result in accountability and responsiveness to business requirements. Building a strong internal control program within IT can help to:

- Gain competitive advantage through more efficient and effective operations;
- Enhance risk management competencies and prioritization of initiatives;
- Enhance overall IT governance;
- Enhance the understanding of IT among executives;
- Optimize operations with an integrated approach to security, availability and processing integrity;
- Enable better business decisions by providing higher-quality, more timely information;
- Contribute to the compliance of other regulatory requirements, such as privacy;
- Align project initiatives with business requirements;
- Prevent loss of intellectual assets and the possibility of system breach.

4 The evolution of the IS auditor profession in the context of changing audit methodologies

In this chapter we present a history of the IS auditor profession and how the status of IS auditors evolved in large financial audit firms. We also try to link this evolution to changes in financial audit methodologies, as presented in chapter 2 of this article.

In [19], the role of information systems auditors in large financial audit firms is examined. The results can be summarized as follows:

Prior to 1990 (financial audit methods were transaction cycle oriented and IS audit was seen as a secondary function to financial audit):

- Most IS auditors were financial auditors with some interest in information systems and many of them fulfilled both roles;
- Firms hired experienced IS professionals when special technology skills were needed for financial audit;
- IS audit was not seen as an added value factor to the audit from either the clients' or the financial auditors' perspective;
- The relationship between financial and IS audit was seen as symbiotic (at least theoretically);
- Financial auditors had little understanding of the work done by IS auditors and were not confident enough of the IS audit risk assessment to consider it into their audit planning;
- IS auditors did not always understand the implications of control weaknesses on financial statements;
- 1990-1995 (BRA methodologies were beginning to be applied by financial audit professionals and new opportunities for selling non-audit services by audit firms arose);
- The emergence and growth of the IS audit practice large audit firms compelled them to hire IS auditors directly;
- IS audit began to achieve some independence as a specialty group that provided certain value-added client services, but still largely supported financial audit;
- IS audit began to shift towards the testing of application controls instead of focusing primarily on an assessment of general controls;
- The firms were beginning to move to automated work papers and were starting to build best practices databases;
- Financial auditors did not see how a weakness in general controls, such as a poor program change control process, affected the financial statements;
- IS auditors were not always able to communicate this impact effectively either, but felt that such a weakness was problematic. As audits shifted more towards a risk-based approach, this understanding gap narrowed;
- 1995-2000 (IS auditors performed manly non-audit services);
- The move toward expanding IS audit services has continued to the extent that financial audit support was less than half of the work done by IS auditors;
- IS auditors were offering a variety of consulting services (e.g. penetration testing, firewall audits, security diagnostics, system effective-

ness, technology assurance, ERP related work and business continuity planning);

- To support the financial audit, general control evaluation work was still being done. However, this work was undertaken only after a risk assessment was made that identified the impact control weaknesses were likely to have on both the client's financial statements and on the overall business.

The increasing importance of non-audit services (including IS audit) is confirmed by the evolution of their weight in the overall revenues of large audit firms (Table 2).

Table 2. FTSE top 100 companies: ratios of audit to non-audit fees earned by the Big (6/5/4/) Audit Firms 1992–2001 [4]

Year	Ratio of non-audit fees : audit fees	Audit fees (%)	Non-audit fees (%)	Total fees (%)
1992	0.2:1	81	19	100
1993	0.6:1	63	37	100
1994	0.6:1	62	38	100
1995	0.6:1	62	38	100
1996	0.9:1	51	49	100
1997	1.3:1	44	56	100
1998	1.5:1	39	61	100
1999	2.3:1	30	70	100
2000	2.9:1	26	74	100
2001	3.7:1	21	79	100

5 Conclusions

According to our research, although authors agree on the shift in audit methodologies, from transaction cycle oriented (TFAs) to business process oriented (BRA or SSA), there is still a debate about how beneficial was the change for the audit profession. In our opinion, this debate offers some interesting possibilities of research, as the efficacy of the BRA methodology is yet to be undoubtedly proven.

We concluded that the COSO Internal Control – Integrated Framework was the starting point for fundamental changes in both financial and IS audit. Besides being the most commonly adopted framework by public companies seeking to comply with the Sarbanes-Oxley regulations, it also led to the development of ”business risk audit” methodologies, which in turn opened up the possibility for IS auditors from large audit firms to provide an extended array of IT consulting services.

We also found that the Sarbanes-Oxley Act had a big impact on IS auditing by imposing stricter regulations regarding internal controls and in our opinion, the SOX regulations should be viewed as an enabler rather than an enforcer in establishing strong governance models.

Finally, our research suggests that there is a direct causality effect between the employment of BRA audit methodologies and the growing importance of IS audit. We propose analyzing the influence of other factors, such as evolutions in technology and changes in the business environment to the IS audit as a research theme.

References

[1] International Auditing and Assurance Standards Board (IAASB), *International Standard on Auditing 200. Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing*, New York, 2009.

[2] ISACA, *CISA Review Manual 2009*, 2008, pp. 15-34.

[3] E. Curtis and S. Turley, “The business risk audit – A longitudinal case study of an audit engagement,” *Accounting, Organizations and Society*, No. 32, 2007, pp. 439–461.

[4] K. Robson, C. Humphrey, R. Khalifa and J. Jones, “Transforming audit technologies: Business risk audit methodologies and the audit field,” *Accounting, Organizations and Society*, No. 32, 2007, pp. 409–438.

[5] J. J. Schultz Jr., J. L. Bierstaker and E. O’Donnell, “Integrating business risk into auditor judgment about the risk of material misstatement: The influence of a strategic-systems-audit approach,” *Accounting, Organizations and Society*, 2009, doi:10.1016/j.aos.2009.07.006.

[6] W. R. Knechel, “The business risk audit: Origins, obstacles and opportunities,” *Accounting, Organizations and Society*, No. 32, 2007, pp. 383–408.

[7] M. E. Peecher, R. Schwartz and I. Solomon, "It's all about audit quality: Perspectives on strategic-systems auditing," *Accounting, Organizations and Society*, No. 32, 2007, pp. 463–485.

[8] International Auditing and Assurance Standards Board (IAASB), *International Standard on Auditing 315. Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment*, 2009, New York.

[9] C. Flint, I. A. M. Fraser and D. J. Hatherly, *Business risk auditing: A regressive evolution? - A research note*, Accounting Forum, No. 32, 2008, pp. 143–147.

[10] W. R. Knechel, S. E. Salterio and N. Kochetova-Kozloski, "The effect of benchmarked performance measures and strategic analysis on auditors' risk assessments and mental models," *Accounting, Organizations and Society*, 2009, doi:10.1016/j.aos.2009.09.004.

[11] C. Dowling and S. Leech, "Audit support systems and decision aids: Current practice and opportunities for future research," *International Journal of Accounting Information Systems*, Vol. 8, 2007, pp. 92–116.

[12] P. Sikka, "Financial crisis and the silence of the auditors," *Accounting, Organizations and Society*, No. 34, 2009, pp. 868–873.

[13] C. Carnaghan, "Business process modeling approaches in the context of process level audit risk assessment: An analysis and comparison," *International Journal of Accounting Information Systems*, Vol. 7, 2006, pp. 170–204.

[14] T. Singleton, "The COSO Model: How IT Auditors Can Use It to Evaluate the Effectiveness of Internal Controls," *Information Systems Control Journal*, Vol. 6, 2007.

[15] Internal Control-Integrated Framework, *Committee of Sponsoring Organizations of the Treadway Commission*, 1992, AICPA, Jersey City, NJ.

[16] T. Singleton, "Emerging Technical Standards on Financial Audits: How IT Auditors Gather Evidence to Evaluate Internal Controls," *Information Systems Control Journal*, Vol. 4, 2007.

[17] R. J. Dietrich, "After Year One - Automating IT Controls for Sarbanes-Oxley Compliance," *Information Systems Control Journal*, Vol. 5, 2005.

[18] IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting*, 2nd Edition, 2006, pp. 27-45.

[19] N. A. Bagranoff and V. P.Vendrzyk, „The Changing Role of IS Audit Among the Big Five US-Based Accounting Firms," *Information Systems Control Journal*, Vol. 5, 2000.

Daniel VÎLSĂNOIU has graduated the Accounting and Management Information Systems Faculty from the Bucharest Academy of Economic Studies in 2008. He is a PhD candidate since October 2008 and his main research areas are: expert systems, information systems audit, financial audit and IT risks and controls.

Mihaela ŞERBAN is a PhD student and a graduate of the Faculty of Accounting and Management Information Systems. She is currently conducting research in Accounting within the Bucharest Academy of Economic Studies. Amongst her fields of interest are corporate governance, financial audit and internal controls.