Characteristics of the Audit Processes for Distributed Informatics Systems

Marius POPA, Cristian TOMA, Cristian AMANCEI
Department of Computer Science in Economics,
Academy of Economic Studies, Bucharest, Romania
marius.popa@ase.ro, cristian.toma@ie.ase.ro, cristian.amancei@ie.ase.ro

The paper contains issues regarding: main characteristics and examples of the distributed informatics systems and main difference categories among them, concepts, principles, techniques and fields for auditing the distributed informatics systems, concepts and classes of the standard term, characteristics of this one, examples of standards, guidelines, procedures and controls for auditing the distributed informatics systems. The distributed informatics systems are characterized by the following issues: development process, resources, implemented functionalities, architectures, system classes, particularities. The audit framework has two sides: the audit process and auditors. The audit process must be led in accordance with the standard specifications in the IT&C field. The auditors must meet the ethical principles and they must have a high-level of professional skills and competence in IT&C field.

***Keywords**: informatics audit, characteristic, distributed informatics system, standard.*

1 Characteristics of the Distributed Informatics Systems

A *system* represents a set of dependent elements forming a single unitary entity. A particular type of system is the *economic* one, which defines economic components and mechanisms such as a company, an industry, a field of the national economy and so on. Even the national and worldwide economies can be seen at a global economic level as being complex economic systems [1].

A system is defined by the following elements: inputs, outputs, transformation process and system structure with its state.

An information system utilizes automatic methods and means for data collecting, transmission, storage and processing for information capitalization in the organization management process [2].

A system is named distributed because its components are placed in different logical and physical locations.

The resources involved by an information technology system can be divided into the following groups [1]:

- *Activity:* it is the subject of the system and the primary data from inside;
- *Methods and techniques:* they are used to develop the distributed informatics system;
- *Hardware:* it is involved in collecting, processing, transmitting, storing and presenting the final results;
- *Software applications:* these are responsible for the efficient use of the hardware resources by finding the solutions for the specific problems;
- *Human resources:* they are very important for the health of the system.
- The automatic data processing covers the collecting, transmitting, processing and storing operations [1]:
- *Collecting data:* takes place at the location where the primary data are generated; all the collected elements are stored in a proper manner to be used to automatic processing;
- *Processing data:* the primary data are transformed into results by following a predefined sequence of operations adapted to the user requirements, hardware specifications and processing technique.
- *Transmitting data:* from the primary locations to the automatic processing systems; also, it is responsible for delivering the final results to the consumers;
- *Storing data:* is responsible for data

archiving on specific medium in order to be possible to access and process the content in the future.

In [3], the informatics system is defined as a set of hardware and software components interconnected in networks, the organizational and administrative framework in which these components are working. The interconnection of these components is made on two levels:

- *Physical level:* it supposes the connection through different devices of the equipments in order to build the system;
- *Functional level:* it is made on the software level as to assure the system functionality through software modules collaboration.

The informatics systems evolved as new IT&C technologies were developed. Therefore, new categories of informatics systems appeared and some examples are [4]:

- *Transaction processing systems:* they automate the handling of data about business activities or transactions;
- *Management information systems:* they are subsets of the overall internal controls of a business to accomplish specific goals or objectives;
- *Decision support systems:* they include knowledge-based systems that support decision-making activities;
- *Expert systems:* they are software products that attempts to reproduce the performance of one or more human experts;
- *Business intelligence:* it refers to skills, technologies, applications and practices used to help a business acquire understanding of its business context.

The distributed informatics systems differ from each other by the following elements [5]:

- Disposition of the components;
- Network topologies and methods of component connection;
- Resources allocated for development;
- Levels or layers within architecture;
- Implemented functions for processing;
- Quality level of the obtained characteristics;
- Cost of development;
- Duration of development.
- The particularities of the distributed informatics systems are [5]:
- Strong interfaces used by different categories of users;
- High generality degree to solve different kind of users' issues;
- Friendly interfaces to eliminate the input data errors and the abandon of the utilization;
- Security levels that guarantee the system of transactions is operational;
- Access levels that solve the security issues with the transparency one in a convenient way;
- High level of correctness and reliability;
- Guarantee for recording sufficient information to reconstitute the information route;
- Components of any distributed informatics system: application and communication; some components contain an administrative part with control role and manage role of components;
- High degree of modularity and extensibility through addition or elimination of some software or hardware components;
- Sharing the resources by many users;
- Large availability in case of fault of some components;
- Fault tolerance.

The general characteristics of a distributed informatics system are [5]:

- Correct functionality of the distributed informatics systems' components in a secure and interoperable way;
- Reliability that maintains the level of application performance for a long period of time; the based attributes of these characteristics are: fault tolerance and recoverability of data affected by different application errors;
- Usability by different users;
- System efficiency given by time and used resource behavior;
- Maintainability that refers to the effort needed for certain modifications;

- Portability that assures the application running on different systems;
- Interoperability with other distributed informatics systems;
- Complexity correlated with other characteristics as reliability, stability or maintainability;
- Flexibility, in the special case of the web distributed applications; from the web server point of view, this characteristic means the capacity to incorporate data from accessed databases in web pages;
- Security that offers a safer way to work with information in a computer network, using specific techniques: security tools for servers, cryptographic support, safer programming techniques, read/write rights, access protected by password etc.

For instance, reliability means the probability of the distributed informatics system to accomplish its functions in the designed parameters. The failures of a distributed informatics system have as possible causes [19]:

- Inappropriate testing of the system;
- Management changes;
- Operating errors;
- Weak source code;
- Lack of quality assurance process;
- Interactions with external applications or services;
- Different operating conditions;
- Random events;
- Hardware failures;
- Environment issues.

The characteristics of the distributed informatics systems are quantified by metrics and indicators.

The reach of the organization goals is also determined through indicators. There are three large indicator classes [18]:

- Success indicators – determining if the goals are met;
- Progress indicators – tracking the execution of tasks;
- Analysis indicators – assisting in analyzing the output of each task.

The particular characteristics of the distributed informatics systems and the way in which these characteristics are met depend of the category in which the distributed informatics system is classified.

For instance, in addition of the implementation cost of an Enterprise Resource Planning – ERP system, there are other hidden costs for such kind of distributed informatics systems, like the following [6]:

- *Training:* basically it is very expensive because workers should learn not only how to use a new software, but also they need to accommodate with new procedures, documents, data flows and so on;
- *Testing*: any new implementation represents a customization of a standard product; all the modules should be tested in order to be sure they are working as expected;
- *Integration:* all the interfaces developed for the communication between the ERP and other systems should be carefully verified; the company who implements the system must be sure no data is lost, corrupted or incorrectly used;
- *Customization:* it represents the adaptation of an ERP system to a particular type of business; the modules are linked together so the changes should be propagated in the whole system; also, it is possible the client to ask for specific add-on, modules, functions that must be paid;
- *Data migration*: it is made from the previous system(s) to the current ERP implementation; data from the past will be migrated to the current system using dedicated procedures that should be developed especially for the current implementation;
- *Consultants and analysts:* they can hardly improve the implementation time but they also increase the costs; to move on from critical situations, the fees for consultants and analysts are very high but the impact of their actions over the system is significant;
- *Post implementation depression:* very often, the ERP implementation initially generates at employees' level a drop in

performance because everything looks different than they know and the things are not familiar anymore; the top and middle management should inform employees about all the benefits coming from the use of the new system in terms of money and efficiency.

Another example of distributed informatics system is Secure Automatic Ticketing System – SATS. SATS has several major objectives:

- to implement the secure use of the electronic cards and tags instead of paper tickets in any kind of information integrated system;
- to supervise the actions and the behavior of the subscribers within the ticketing system in order to prevent the frauds and to increase the subscribers' and clients' satisfaction;
- to improve the management of the company, providing complete and proper information about the components of the system;
- to improve the commercial offers to the subscribers and clients;
- to improve the quality of the commercial services.

SATS is inspired as terminology from the mobile applications environment and it is designed for contactless integrated circuits cards with memory chip.

The SATS handles pre-pay, post-pay and both client types. In addition, SATS has the availability to works with e-Cards as well as with paper tickets. The clients who buy paper tickets are considered pre-pay clients. For a better view about of the client types, they are presented in figure 1.

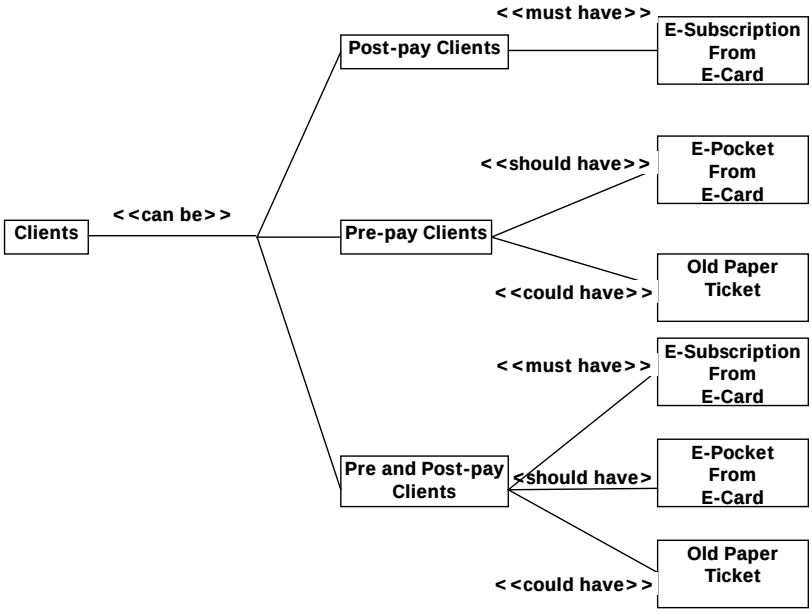

Fig. 1. SATS Client Types

Table 1. Correlation between IT strategy and business strategy

	Very poor	Poor	Avg.	Good	Very good
IT management	1%	6%	32%	44%	16%
Audit	0%	20%	0%	60%	20%
CIO	0%	2%	31%	48%	19%
General management	0%	0%	28%	39%	33%

The ideal case all the SATS clients are not using old paper ticket. In order to validate the E-Subscription or E-Pocket, SATS uses E-Validation devices.

Table 2. Evolution of the IT importance

	2003	2005	2007
Not important at all	1%	0%	0%
Not very important	1%	3%	1%
Not sure	7%	10%	6%
Somewhat important	39%	30%	30%
Very important	52%	57%	63%

It must be a correlation between the business

strategy and IT strategy within organization. Depending on respondent's position, in [17] this correlation is presented as in the table 1.
The importance degree of IT to the business strategy is increasingly more as it is depicted in [17] and it is highlighted in the table 2.
The contributions of IT by sectors to the overall business strategy are depicted in the table 3.

Table 3. Contributions of IT by sectors to the business strategy [17]

	NIA	NVI	NS	SI	VI
IT/telecom	4%	0%	0%	25%	71%
Financial services	0%	0%	2%	20%	77%
Manufacturing	7%	3%	0%	35%	55%
Retail	4%	1%	0%	32%	63%
Public sector	5%	1%	0%	33%	61%
Other	5%	2%	0%	29%	61%

where:
- NIA – Not Important at All;
- NVI – Not Very Important;
- NS – Not Sure;
- SI – Somewhat Important;
- VI – Very Important.

The communication from IT to the business is very important to reach the organization goals. In [17], there is depicted a chart about the evolution of this communication as it is show in the table 4.

Table 4. Evolution of the communication between IT and business

	2005	2007
Never	7%	4%
Sometimes	38%	36%
Regularly	41%	41%
Always	14%	18%

All above statistics demonstrates that the influence degree of the IT to the business strategy is more important and complex. This is another reason to carry out audit processes on IT&C processes, management and products to increase the accomplishment degree of the organization goals established by management.

2 Principles of the Informatics Audit Processes

The *audit* concept was taken over from Angle-Saxon countries. In its classical form, the concept is linked of financial and accounting domain and it refers to financial reports of a company. In these countries, there are legal regulations regarding the audit constraint for the all stock companies.
Through the fact that in many other domains examinations and objective, impartial and independent evaluation are necessary, the audit concept was taken over and adapted for many other domains, including the informatics field.
The *audit* term comes from the Latin *word* = *listening.* As listening demarche, then inquest and solution suggestion in final, the audit permits the supply of explained and independent reasoning.
The *audit* is the process through competent and independent persons collect and evaluates proofs to set an opinion on correspondence degree among the observed things and some pre-defined criteria [7].
The Anglo-Saxon literature terminology includes the following concepts of the audit in Information Society [7]:
- *Audit of Information Systems* – it refers to information system evaluation, practices and operations of this one;
- *Audit of Computer Information Systems* – has the same meaning as information system audit, in an environment based on computer use;
- *Computer Auditing* – has more meanings: the computer use as audit tool, audit in an environment based on computer use or special investigations, connective with financial audit.

The concepts used in French literature are [7]:
- *audit informatique – informatics audit* – supposes the applying of a quality label on an object in regards to referent system;
- *audit des systèmes d'information – information system audit* – consists of coherence evaluation, quality and security of informatics security, that is of the importance for informatics risks and comprehension and efficacy testing of the control, prevention and protection means.

The informatics system audit developed

reason of computation technique getting through the most part of financial and accounting operations. At the start, it was about a simple copying of manual operations, inputs and outputs being audited. The next developments in computing technique, programming languages, programming techniques and data management systems determined an important change of conception. Thus, the audit is made through computer [7].

The distributed informatics systems are complex constructions. They are designed, implemented and maintained to resolve different business tasks in companies. Having in mind the human and financial resources consumption to develop a distributed informatics system, it is necessary to carry out some activities that lead to proposed objective. Also, the proposed objective must be reached in time with the established quality level and within the budget limits [8].

In [9], it is formalized the sense to be of the audit in a series of postulates or supposes that are deduced from audit function existence. The audit postulates are grouped in:

- *Justificative postulates*: justifies the necessity of audit achievement;
- *Behavioral postulates*: statuettes the relations auditor – audited organization and auditor statute;
- *Functional postulates*: it refers to the following aspects:
  - Audit activity achievement with a reasonable cost and in a reasonable period of time;
  - Protection assurance against frauds and errors;
  - Correct and fair concepts defined in terms of accounting methods.

The justificative postulates are accepted without reserves. The most important part of the debates in literature regarding the audit focuses on behavioral postulates, in particular on independence, and auditor experience in fields as sampling in statistics, informatics accounting audit and fraud detection. The debates on postulates tend to develop in financial accounting field.

There are models of auditors' roles. These ones are derived from role theory in which the sociologists consider the position of each person in society is determined by the expectations or society standards [7].

Principles that underlie the audit process are:

- *Independence*: freedom to develop the audit program by auditors, to examine the information deemed to be relevant and the contents of the report are related to the scope of examination;
- *Use of audit evidence*: it is the information that an auditor uses it for underling the conclusions and to draw up the audit report.
- Principles that the auditors must follow are:
- *Ethical behavior*: it is governed by independence, integrity, objectivity, professional competence, confidentiality, professional behavior and technical standards; in [10], there is defined a Code of Professional Ethics for members and certification holders who must meet the following requirements: audit compliance with standards, guidelines and procedures, professional care in accordance with professional standards and best practices, serving in the interest of stakeholders, maintaining the privacy and confidentiality, developing the activities in accordance with professional competence, informing of the appropriate parties, supporting the professional education of stakeholders;
- *Correct reporting*: it is written by persons with professional skills and high experience in the audited field; the content is based on audit evidences, information recommendations for the audit client;
- *Professional responsibility*: auditors have the obligation to respect the principles of the audit process and to assume the consequences if they don't do that.

Audit techniques are standardized, supplying the necessary elements that cover a large spectrum of the topics, beginning with auditors' employment and finishing with audit report editing and presentation.

It was established the following categories [8]: general, performance and work and reporting standards.

The audit techniques are implemented by persons with studies in the field, ability for this control, with adequate experience. The auditors are independents and honest, they hold a professional exam, they have university courses and they have a good and long professional practice. These aspects give sufficient experience in chosen field, inclusively in juridical one. The auditors have a distinct professional statute, being identified three big categories [8]:

- Independent auditors – perform the service for a certain client for a fee; on the base of activity carrying out is the concept of independence auditor;
- Internal auditors – are employees of the organization, assisting the company staff to accomplish their responsibility;
- Governmental auditors – are employees of different governmental agencies; also, their activity consists of work conformity with the established laws and rules, the using way of the resources, the governmental department efficiency.

IT&C technologies used to develop distributed informatics systems are faster, smaller and cheaper. The climate of the IT&C technologies is in a constant and rapid change. Thus, the informatics audit must face new challenges due to the characteristics of the modern distributed informatics systems. Also, the informatics audit requires a dynamic and flexible control structure [11].

One of these activities, very important both for developers and users, is the informatics audit process. Informatics system audit is a branch of general audit that attends with information and communication technology control [3].

The general term of the audit process is defined as: "The independent examination of records and other information in order to form an opinion on the integrity of a system of controls and recommend control improvements to limit risks" [12]. This definition includes some key words, having the following significances applied to the informatics audit:

- *Independent*: audit process is developed by auditors who are not involved in the operations or management of the audited processes; the auditors gather the facts and observe situations objectively; also, they report the results to a separate line of the management;
- *Examination*: results of the audit process are traceable to valid information sources;
- *Records and other information*: review process of the system is based on information gathered from the audited system;
- *Opinion*: auditors present the objective facts and subjective opinions on the state of the reviewed system; the subjective opinions are based on the interpretation of the facts identified within system;
- *Integrity*: it is defined by other tree terms to highlight the mean of this one; the terms are: completeness, accuracy and trustworthiness;
- *System of controls*: different types of control operate to many levels: technical controls built-in to the informatics systems, procedural controls, legal controls, human resources controls; these controls are classified in the following groups: preventive, detective, or corrective controls;
- *Recommend*: auditors elaborate audit recommendation to the management; they have not the authority to implement the suggested changes and they cannot force the management to do so; auditors achieve the implementation of the recommendation through processes of explanation, justification and persuasion, explaining the risks and justifying the need to apply the changes;
- *Control improvements*: it supposes the addition of the controls that were missing, improving the controls that are in place and removing of the ineffective or wasteful controls;
- *Limit*: it refers to reducing, minimizing the risks; the risks cannot be eliminated, but they can be evaluate to reach the

proposed objective;
- *Risk*: possibility that something wrong to appear; it is a combination of threats, acting on vulnerabilities.

A perspective regarding the informatics audit is offered in [12]. Thus, "An IT Auditor often is the translator of business risk, as it relates to the use of IT, to management, someone who can wade through the technical morass well enough to understand the risk (not necessarily manage the technology) and make a sound assessment and present risk-oriented advice to management. The key word is translator, someone capable enough in business strategy and policy and in technology to provide a sound assessment of the risk environment."

An IT&C system differs of a manual one through the way in which the results are obtained, the level of security and control, the risks associated to the processing. The potential impact of the risks is minimized through high standards of security and control.

In [11], there are presented some common instances of computer fraud and abuse:
- Unauthorized disclosure of confidential information;
- Unavailability of key IT&C systems;
- Unauthorized modification/destruction of software;
- Unauthorized modification/destruction of data;
- Theft of IT&C hardware and software;
- Use of IT&C facilities for personal business.

Audit is more that compliance. Compliance is management's day job and it aims the compliance of the system with the rules described in policies, standards and procedures internally generated or laws, regulations and contractual terms as externally requirements. Audit checks whether the management processes to achieve the compliance are effective and that the rules are suitable and sufficient.

The main fields in which the informatics audit is developed are [11]:
- *Systems under development*: development of a new informatics system represents a significant risk for an organization; the new system must meet a large variety of business needs, new legal requirements, maintaining and enhancing the profitability, improving the efficiency, reducing the costs;
- *Live applications*: IT&C systems running within organization must be periodically evaluated; the reasons for a periodic evaluation of the applications are: dynamically changes of the IT&C applications, change of the control environment, additional security and control for data, change of the risks and its impact on the security and controls;
- *IT&C infrastructure*: it refers the hardware, software and communication components of an informatics system; also, it represents an area of significant risks because the business applications are dependent upon the level of integrity, availability and confidentiality within the IT&C infrastructure;
- *Audit automation*: core activity of some IT auditors; it is used to obtain independent data from the system; it must be considered under two main headings: an audit tool and an administration tool.
- The way in which an audit is performed depends of organization and auditor. Each of these has an own way to perform the audit.
- The main stages of an audit process that can be identified are described in [12]:
- *Scoping and pre-audit survey*: it determines the main areas of focus and out of scope on risk-based assessment;
- *Planning and preparation*: the scope is broken down into greater levels of detail, generating an audit work plan and risk-control-matrix;
- *Fieldwork*: evidence are gathered by interviews, document reviewing, Computer Aided Audit Techniques – CAAT use;
- *Analysis:* some analysis techniques like SWOT (Strengths, Weaknesses, Opportunities, Treats) and PEST (Political, Economic, Social, Technological) are used to associate a

sense to the gathered evidence;
- *Reporting:* an audit report is elaborated after many reviews and revisions in order to issue it;
- *Closure:* preparing the notes and future audits; also, the management must be convinced to apply the measures proposed by the audit team in the report.
- The main types of IT&C audits are described in [12]:
- *Operational computer system or network audits*: audit aims the operational informatics system and network at various levels: network, operating systems, layered software, application software, databases, logical/procedural controls, cryptography, logging etc;
- *Audits of IT&C installation*: they aim physical security, environment control, computer and network operations processes and management systems etc;
- *Audits of system development*: controls of project/programme management, technical and procedural controls for specification, development, testing, implementation and operation of the informatics systems;
- *Audits of IT&C management*: there are reviewed organization, structure, strategy, work planning, resource planning, budgeting, cost controls and relationships with outsourced IT providers;
- *IT&C process audits*: review IT&C processes as application development, testing, implementation, operations, maintenance, housekeeping, support, incident handling;
- *Change management audits*: aim the planning and control of changes to systems, networks, applications, processes, facilities etc;
- *Information security and control audits*: confidentiality, integrity and availability of the systems and data are reviewed within this kind of audits;
- *Audits for IT&C legal compliance*: legal and regulatory aspects of the IT&C systems are reviewed;
- *Audits for compliance and certification*: are conducted by auditors from accredited certification bodies; they reviewed the compliance with the information security standards and can grant a certificate to the audited organization;
- *Audits for disaster contingency, business continuity planning or disaster recovery*: review the returning to the normality after a disaster affected the IT&C systems; also, they can assess the organization's approach to risk management;
- *IT&C strategy audits*: IT&C strategy, vision and plans are reviewed;
- *Special investigations*: are unplanned activities to investigate suspected frauds or information security breaches.

The distributed informatics systems are increasingly complex systems with a wide range of architectures, structures and components. In addition, the IT&C technologies are more complex and heterogeneous. These facts together with legal requirements have determined to evaluate such systems through audit performing in compliance with standards, guidelines and procedures elaborated by international standardization organizations.

3 Audit Standards for Distributed Informatics Systems

In IEEE vision, the a*udit* represents an independent evaluation of software products or processes that assure the consonance with the standards, guiding lines, requirements and procedures based on objective criteria [8].

The audit standard contains mandatory requirements from auditors' employment to drawing up and presentation of the audit report. There are the following general classes of standards [7]: general, performance and reporting standards.

Depending on the geographical coverage, the standards are national or international.

If the covered activity field is considered, then standards are classified in:
- Standards of the companies;
- Standards of an industry.

In the audit processes of the distributed informatics systems, standards are used to the following levels:

- IT&C resources and processes;
- Information security;
- IT&C security.

ISACA – Information Systems Audit and Control Association, developed a document having the title IS Standards, Guidelines and Procedures for Auditing and Control Professionals in order to highlight the way in which these ones are accomplished [6].

In according with [10], in the below section, the concepts of standard, guideline and procedure are defined:

- *Standards*: define mandatory requirements for informatics system auditing and reporting; they take into account the following elements:
  - The informatics system auditors must be in accordance with the professional responsibilities set out in the ISACA Code of Professional Ethics for information system auditors;
  - Management and other interested parties;
  - Holders of the Certified Information Systems Auditor™ designation of requirements;
- *Guidelines*: provide guidance in applying standards for informatics system auditing; the auditor should consider the guidelines in order to determining how to achieve implementation of the standards, use professional judgment in their application and be prepared to justify any departure;
- *Procedures*: provide examples of procedures an informatics system auditor might follow in an audit engagement; the procedure documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements.

ISACA information system audit standards contain basic principles and essential procedures that are mandatory together with related guidance.

CobiT framework has to be used as a source of best practice guidance. CobiT includes set of controls and control techniques for information system management. In the IT&C audit processes, it must select the appropriate elements from CobiT in order to evaluate IT&C processes and consideration of information criteria.

The CobiT framework is based on the following principles [13]:

- Business Requirements of the enterprise need investments in IT Resources;
- IT Resources are used by IT Processes;
- IT Processes perform services that deliver Enterprise Information;
- Enterprise Information respond to Business Requirements of the enterprise.

Business and IT&C management and information system auditors can use CobiT that includes [10]:

- *Control Objectives*: represents high-level and detailed generic statements of minimum good control;
- *Control Practices*: contain "how to implement" guidance for the control objectives;
- *Audit Guidelines*: regard the understanding and evaluation of each control, assess compliance and substantiate the risk of controls not being met;
- *Management Guidelines*: regard the assessment and improvement of IT process performance, using maturity models, metrics and critical success factors; it provides a management-oriented framework for continuous and proactive control self-assessment specifically focused on:
  - Performance measurement: support degree in which the IT function supports business requirements, self-assessment workshops, continuous monitoring and improvement procedures;
  - IT control profiling: importance degree of IT processes, identifying the critical success factors for control;
  - Awareness: establishing the risks of not achieving the objectives;

– Benchmarking: third parties work, measurement and comparison of the results, metrics enabling assessment of IT performance in business terms, key goal indicators, outcomes of IT processes, and the key performance indicators; assessment and benchmarking help management to measure control capability and to identify control gaps and strategies for improvement.

The ISACA document contains the following auditing standards of the information systems [10]:

- S1 Audit Charter
- S2 Independence
- S3 Professional Ethics and Standards
- S4 Competence
- S5 Planning
- S6 Performance of Audit Work
- S7 Reporting
- S8 Follow-Up Activities
- S9 Irregularities and Illegal Acts;
- S10 IT Governance
- S11 Use of Risk Assessment in Audit Planning
- S12 Audit Materiality
- S13 Using the Work of Other Experts
- S14 Audit Evidence

Each of the above ISACA standards is detailed in four sections: introduction, standard, commentary and operative date. For instance, standard S7 Reporting contains specifications about the following aspects [10]:

- Report has an appropriate form, upon completion of the audit, identifies the organization, the intended recipients and any restrictions on circulation;
- Report states the scope, objectives, period of coverage and the nature, timing and extent of the audit work performed;
- Report states the findings, conclusions and recommendations and any reservations, qualifications or limitations in scope that the IS auditor has with respect to the audit;
- Auditor has to have sufficient and appropriate audit evidence to support the results reported;
- Report has to be signed by auditor, dated and distributed in accordance with the audit charter or engagement letter.

The standard S7 Reporting is supported by following sources of guidance and additional information:

- Information System Guideline G20 Reporting;
- CobiT Framework, Control objective M4.7 and M4.8.
- In ISACA information system audit, 35 IS auditing guidelines are defined. Each guideline is detailed on many levels. For instance, the G2 Audit Evidence Requirement has the following levels [10]:
  - *Background*: linkage to standards, need for guideline;
  - *Planning*: types, availability and selection of audit evidence;
  - *Performance of audit work*: nature of audit evidence, gathering audit evidence, audit documentation;
  - *Reporting*: restriction of scope;
  - *Effective date*: beginning date of the guideline.

Other specifications regarding the distributed informatics systems are included in international standard ISO/IEC 17799 – Information Technology – Security Techniques – Code of Practice for Information Security Management. This international standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization [14].

The following controls are considered to be common practice for information security, as they are defined in [14]:

- Information security policy document;
- Allocation of information security responsibilities;
- Information security awareness, education, and training;
- Correct processing in applications;
- Technical vulnerability management;

- Business continuity management;
- Management of information security incidents and improvements.
- ISO/IEC 17799 International Standard contains 11 security control clauses [14]:
- Security Policy (1);
- Organizing Information Security (2);
- Asset Management (2);
- Human Resources Security (3);
- Physical and Environmental Security (2);
- Communications and Operations Management (10);
- Access Control (7);
- Information Systems Acquisition, Development and Maintenance (6);
- Information Security Incident Management (2);
- Business Continuity Management (1);
- Compliance (3).

The number that accompanies each clause represents the number of main security category included within the clause. Each main security category includes:

- A control objective stating what is to be achieved;
- One or more controls that can be applied to achieve the control objective.
- For instance, one of the security controls aims the user accounts. The auditor must obtain information regarding the following issues:
- Account name;
- Disable state;
- Locking state;
- Expiration of the password;
- Requiring of the password;
- Expiration of the account;
- Last logon (days);
- Logon hours;
- Password age (days);
- Days to the password expiration (days);
- Excessive password life.

Another international standard is ISO/IEC 27001 – Information Technology – Security Techniques – Information Security Management Systems – Requirements. This international standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System – ISMS within the context of the organization's overall business risks [15].

In accordance with [15], the Plan-Do-Check-Act PDCA model applied to Information Security Management Systems processes has the following characteristics:

- *Plan*: establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security;
- *Do*: implement and operate the ISMS policy, controls, processes and procedures;
- *Check*: assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience;
- *Act*: take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information.

The audit of distributed informatics systems permits their quality level evaluation. Human subjects who must be independent and have a very good professional background and skills in order to lead the audit process make the evaluation in accordance with the audit standards and best practices developed by the biggest organization for standardization.

4 Conclusions

The audit process consists in establishing the degree in which an evaluated system is concordant with the requirements formulated by the target group. Also, the audit process has as result an assessment of the performance of the evaluated system.

In order to assure the business requirements, the management invests in informatics systems. The evolution of the IT&C technologies and geographical expansion of the companies conducted to the development of a new kind of informatics systems: the distributed ones.

The audit process of a distributed informatics system is led by professional personal in IT&C field in accordance with the international standards elaborated by professional organizations. To do that, the

IT&C auditors must have a high level of professional skills and competence. Also, they must follow a permanent training in the field to face new challenges of the IT&C technology changes.

In this context, this paper presented the audit framework for auditing the distributed informatics systems, taking into account the specific characteristics for this kind of systems. Also, the paper highlighted the standardization issues of the auditing processes. These issues are critical to perform high-level quality approach in auditing processes.

The paper was elaborated within the research project with code 1838/2008, contract no. 923/2009 and the title *Implementation of the Quantitative Methods in Distributed Informatics System Audit*, financed by The National University Research Council – Ministry of Education, Research and Innovation from Romania.

References

[1] M. Popa, F. Alecu and C. Amancei, "Characteristics of the Audit Process for Information Systems", in *Proc. The Proceedings of the International Conference Competitiveness and European Integration – Business Information Systems & Collaborative Support Systems in Business*, Cluj-Napoca, October 26 – 27, 2007, Risoprint Printing House, Cluj-Napoca, pp. 295 – 299

[2] M. Popa, "Detection of the Security Vulnerabilities in Web Applications", *Informatica Economică*, vol. 13, no. 1, pp. 127 – 136, March 2009, www.revistaie.ase.ro

[3] I. Ivan, G. Noşca and S. Capisizu, *Auditul sistemelor informatice*. Bucharest: ASE Publishing House, 2005

[4] http://en.wikipedia.org/wiki/ Information _system

[5] E. Dumitraşcu and M. Popa, "Evaluating the Effects of the Optimization on the Quality of Distributed Applications", *Journal of Applied Quantitative Methods*, vol. 2, Issue 1, pp. 70 – 82, March 2007, www.jaqm.ro

[6] M. Popa and F. Alecu, "ERP Informatics System Audit", *Informatica Economică* 2nd supplement „Knowledge Management – Projects, Systems and Technologies: Reinforcement and Extension of Universities & Business Community Partnerships in the Knowledge Era", vol. 10, pp. 109 – 116, November 2006

[7] S. Capisizu, "Models and Techniques for Development the Economic Information Audit", ASE Bucharest, 2006, PhD Thesis

[8] S. Capisizu, G. Noşca and M. Popa, „Informatics Audit", in *Proc. The 37th International Scientific Symposium of METRA*, Military Equipment and Technologies Research Agency, Bucharest, May 25 – 26, 2006

[9] R. Mautz and H. Sharaf, "The Philosophy of Auditing", American Accounting Association, 1961

[10] Information Systems Audit and Control Association, "IS Standards, Guidelines and Procedures for Auditing and Control Professionals", 7th of September, 2006

[11] Barclay Simpson Recruitment Consultant, "An Introduction to Computer Auditing", London, www.barclaysimpson.com

[12] G. Hinson, "Frequently Avoided Questions About Computer Auditing", http://www.isect.com/html/ca_faq.html

[13] IT Governance Institute, "CobiT 4.1, Framework – Control Objectives – Management Guidelines – Maturity Models", 2007

[14] International Standard "ISO/IEC 17799, Information Technology – Security Techniques – Code of Practice for Information Security Management", Second Edition, 2005

[15] International Standard "ISO/IEC 27001, Information Technology – Security Techniques – Information Security Management Systems – Requirements", First Edition, 2005

[16] M. Popa, M. Florescu, and C. Bodea, "Information System Quality Evaluation

Based on Audit Processes", in Proc. *Proceedings of the 2008 International Conference of Information Engineering*, Newswood Limited, International Association of Engineers, Imperial College London, July 2 – 4, 2008, pp. 494 – 496

[17] IT Governance Institute, "IT Governance Global Status Report – 2008", ITGI, 2008

[18] W. Goethert, W. Hayes, "Experiences in Implementing Measurement Programs", Software Engineering Measurement and Analysis Initiative, Technical Note, November 2001

[19] I. Ivan, M. Popa, "Entități text", ASE Printing House, Bucharest, 2005

Marius POPA has graduated the Faculty of Cybernetics, Statistics and Economic Informatics in 2002. He holds a PhD diploma in Economic Cybernetics and Statistics. He joined the staff of Academy of Economic Studies, teaching assistant in 2002 and lecturer in 2006. Currently, he is lecturer in Economic Informatics field and branches within Department of Computer Science in Economics at faculty of Cybernetics, Statistics and Economic Informatics from Academy of Economic Studies. He is the author and co-author of 6 books and over 100 articles in journals and proceedings of national and international conferences, symposiums, workshops in the fields of data quality, software quality, informatics security, collaborative information systems, IT project management, software engineering. From 2009, he is a member of the editorial team for the *Informatica Economica Journal* and between 2003 and 2008 he was a member of the editorial team for the journal *Economic Computation and Economic Cybernetics Studies and Research.*

Cristian TOMA has graduated from the Faculty of Cybernetics, Statistics and Economic Informatics, Economic Informatics specialization, within Academy of Economic Studies Bucharest in 2003. He has graduated from the BRIE master program in 2005 and PhD stage in 2008. In present, he is lecturer at Economic Informatics Department and he is member in research structures such as ECO-INFOSOC. Since the beginning – 2005 – he is scientific secretary of IT&C Security Master Program from Academy of Economic Studies from Bucharest, **www.ism.ase.ro**. For the International Conference on Economic Informatics, editions 2005 and 2007, he was member of organization committee. His research areas are in: distributed and parallel computing, mobile applications, smart card programming, e-business and e-payment systems, network security, computer anti-viruses and viruses, secure web technologies and computational cryptography. He is teaching object oriented programming, data structures, distributed applications development, viruses and anti-viruses technologies, e-payment systems development and advanced programming languages in Economic Informatics Department and IT&C Security master program. He has published 2 books and over 30 papers in indexed reviews and conferences proceedings.

Cristian AMANCEI is Assistant at Academy of Economics Studies Bucharest, Faculty of Economic Cybernetics, Statistics and Informatics. He is a PhD candidate from October 2007 at Economic Informatics Department from Academy of Economic Studies. He holds a Master in Science – Computerized Project Management from Academy of Economic Studies, Bucharest. He is Certified Information Systems Auditor (CISA). He graduated in Economic Informatics at Faculty of Economic Cybernetics, Statistics and Informatics in 2006. His main research areas are: information system audit, data structures, metrics in information systems, IT controls and IT risks.