JOURNAL OF APPLIED QUANTITATIVE METHODS

STAGES FOR THE DEVELOPMENT OF THE AUDIT PROCESSES OF DISTRIBUTED INFORMATICS SYSTEMS[1]

Marius POPA[2]
PhD, University Lecturer, Department of Computer Science in Economics, University of Economics, Bucharest, Romania

E-mail: marius.popa@ase.ro

Cristian TOMA[3]
PhD, University Lecturer, Department of Computer Science in Economics, University of Economics, Bucharest, Romania

E-mail: cristian.toma@ie.ase.ro

Abstract: *The paper presents elements regarding the way in which an audit process is carried out. The following issues are highlighted: audit concept, audit process flow, audit program and audit program management, classes of audit processes, audit process stages and activities, documents used to conclude an audit process. In this paper, the audit concept is defined together with its characteristics and it is described as activities flow in which there are some stages and steps that must be passed in an audit process. The audit program term is presented together with stages followed in such program management. The paper contains classifications of the audit processes depending on many criteria and it offers some details about the audit process classes. The audit process must be rigorously carried out in accordance to stages established by audit specialists and included in standardized documents. During the audit process, the audit team members generate and fill in some documents and forms to support the audit report. The conclusions included in the audit report are based on audit evidences and observations obtained in audit process.*

Key words: *Audit process; audit stages; distributed informatics system*

1. Characteristics of the informatics audit processes

In accordance with (ISO 19011, 2003), the concept of *audit* means a systematic, independent and documented process to obtain audit evidences and their examination with impartiality to establish the degree in which the audit criteria are met. The examination is

made by persons having specific qualifications who are independent in relation to audit process.

The audit evidences are represented by records, declarations about facts or other information relevant in relation to audit criteria. They are evaluated quantitatively or qualitatively.

The audit criteria represent a set of policies, procedures and requirements.

One or more audit processes compose an audit program. The audits included in an audit program are planned during period of time and they are oriented to a specific purpose. The process flow for management of an audit program is depicted in figure 1 (ISO 19011, 2003).

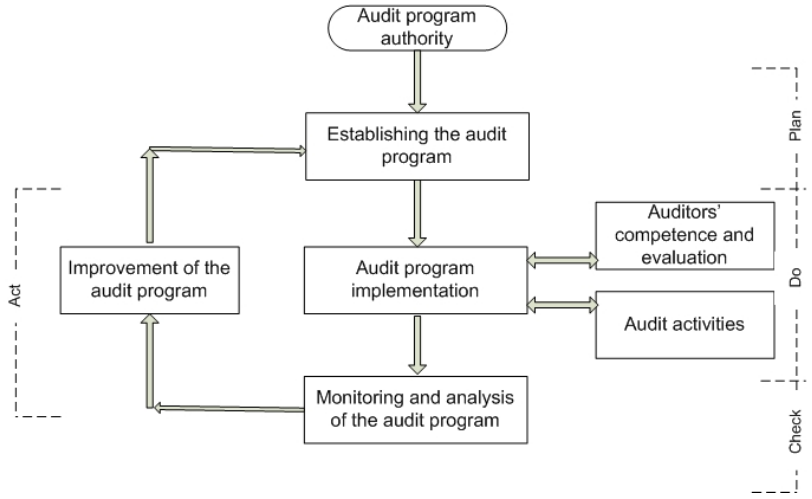

Figure 1. Process flow for audit program management

An audit program contains activities which:

- Plan and organize different audit processes as types and numbers;
- Supply resources for efficacy and efficient execution of the audits in planned interval.

The stage for establishing the audit program includes activities regarding the following issues:

- Purposes and scope – anticipated outcome and amplitude of the audit program are determined by size, type and complexity of the audited organization;
- Responsibilities – they are assigned to persons who understand the audit principles, auditors' competencies and applying the audit techniques; these persons must have management skills and understanding of the technical issues in a business;
- Resources – they are the support of the audit program and there are financial, economic and time ones;
- Procedures – they specify operations arranged in a step-by-step method followed to reach the purpose.

The stage for audit program implementation contains the following activities:

- Audit programming – it refers to the activities regarding the coordination and programming of the audits;

- Auditors' evaluation – it aims the permanent professional improvement and auditors' evaluation;
- Audit team selection – persons with professional skills in audit process are included in audit team;
- Audit activity management – it refers to all activities regarding the audit carrying out;
- Records maintenance – it is useful to demonstrate the audit program implementation and the following records are included: records for each audit, results of the audit program analysis and records regarding personnel used in audit process.

The stage for monitoring and analyzing the audit program contains activities regarding:

- Monitoring and analysis – accomplishment of the objectives is assessed at some intervals; also, some performance indicators are used to determined the accomplishment degree;
- Identifying the need for corrective and preventive actions – it results from monitoring and analysis;
- Identifying the improvement opportunities – it results from the outputs of the audit program analysis.

Audit program management is in accordance with the steps of Deming cycle: Plan-Do-Check-Act (PDCA):

- Plan – objectives, relevant procedures and audit methods are selected and it assigns responsibilities and it allocates resources;
- Do – it refers to audit program implementation, audit team selection, auditors' evaluation, audit execution, records achievement and their maintenance;
- Check – executed activities are monitored and analyzed, corrective and preventive actions and continuous improvement opportunities are identified;
- Act – continuous improvement actions through applying the successful actions and continuing with corrective and preventive actions.

In (ISO 19011, 2003), some examples of audit programs are presented:

- Internal audits – cover all quality management system;
- Second party audits – cover management system of the potential suppliers;
- Certification audits – carried out by third party certification organizations.

Depending on audit place, the following audit classes are identified (ISO 19011, 2003):

- Internal audits – they are led by audited organization to make management analysis or internal reasons or requirements; they are called first party audits and they represent the base for compliance declaration;
- External audits – they include the second and third party audits; second party audits are led by organizations, like clients, that have interests in the audited organization; third party audits are made by external and independent organizations that make audits to certificate the compliance of the audited organization in relation to a standard.

The audit process is developed for more purposes (Floarea Baicu, 2003):

- Initial point – audit process is the initial point to develop a management system;
- Compliance/Noncompliance – audit process establish the compliance of the management system to the requirements;
- Efficacy – audit process establish the efficacy of the management system in relation to objectives of organization;
- Critical points – the audited organization can identify its vulnerabilities and critical point and it can improve the system;
- Measure applying – audit process leads to measure applying to prevent and correct the system and to follow up the applying procedures.

Depending on audit purpose, it can identify the following audit classes (Floarea Baicu, 2003):

- Audits for establishing the situation in a time point;
- Audits for accreditation;
- Audits for certification.

The audit scope classifies the audits in the following classes (Floarea Baicu, 2003):

- Audit of the management system;
- Audit of the process;
- Audit of the product or service.

The audit process is based on principles. A principle represents a basic generalization that is accepted as true. A principle can be used as a basis for reasoning or conduct.

The audit principles provide relevant and sufficient conclusions and they offer the possibility to different auditors who work independently to get to similar conclusions in similar circumstances.

The following principles regard the auditors (ISO 19011, 2003):

- Ethical behavior – it represents the base of professionalism and its characteristics are confidence, integrity, confidentiality and discretion; an auditor has an ethical behavior if the professional standards are met;
- Correct presentation – audit results like observations, conclusions and reports are sincerely and exactly presented to the audited client; also, problems and divergent opinions during the audit process are to be reported; it means the obligation of the audit team to report the results sincerely and exactly;
- Professional responsibility – auditors acts in accordance with their task importance and confidence granted by audit clients; it means the applying of perseverance and audit judgment taking into account the necessary competence;
- Independence – auditor are not influenced by the other audit parts and conflicts of interest; they must have objectivity during the audit process and they base only on evidences to establish the audit observations and conclusions; it represents basis of audit impartiality and objectivity of the audit conclusions;
- Approaching based on evidences – credibility and repeatability of the conclusions are the results of the approaching based on evidences; it means the rational way in which the systematic audit process get to results and conclusions; audit

process is developed in a limited interval and it has limited resources, so the confidence in audit conclusions is given by the confidence in sampling techniques.

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

2. Flow of activities carried out in an audit process of distributed informatics systems

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

An informatics system uses automatic methods and means for data collecting, transmission, storage and processing for information capitalization in the organization management process (Marius Popa, 2009, pp. 127 - 136).

The informatics system resides in all the informational flows and circuits and all the methods, techniques used to process the data necessary to the decision system. The informatics system is the middle layer between the decision and informational systems. The communication between these layers is made in all possible directions. Also, it records, processes and transmits the information from the operational system to the decision one (Marius Popa, 2009, pp. 127 - 136).

A distributed informatics system is a component of the informational system. This kind of informatics system collects, processes, transmits, stores and presents data by using computing systems. Also, it is responsible for automatic processing of the data by using various methods and techniques (Marius Popa, 2009, pp. 827 - 832). An informatics system is called distributed because its components are placed in different logical and physical locations.

In (Ion Ivan, 2005), the distributed 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 following stages of the audit process are described in a general manner in (ISO 19011, 2003). This audit procedure can be applied to all kinds of informatics systems because its description is independent in relation to different kinds of informatics system architectures.

The typical activities of an audit process are depicted in figure 2, including the audit process of distributed informatics systems (ISO 19011, 2003).

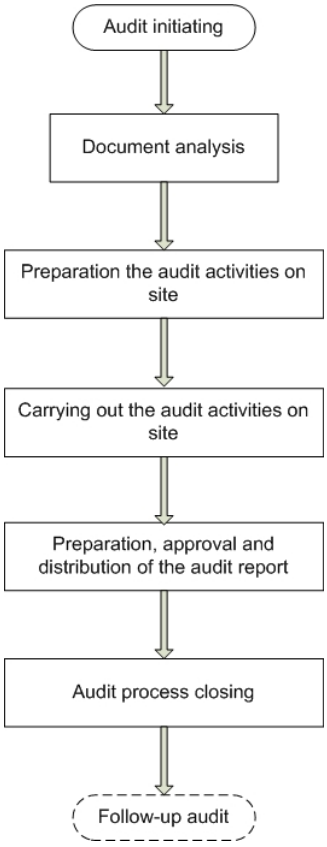

Figure 2. Activity flow in an audit process

Audit initiating contains the following activities (ISO 19011, 2003):

- Audit team leader' assignment – it is made by the persons responsible for audit program management;
- Defining the objectives, purpose and audit criteria – the objectives include: compliance degree of the auditee's management system in relation to audit criteria, capability of the management system to assure the compliance, evaluation of the management system efficacy, identifying the improvement opportunities; audit scope describe the amplitude and boundaries like physical locations, organizational units, audited activities and processes, period of time allocated for audit; audit criteria are used as reference to establish the compliance; they include policies, procedures, standards, law and regulations, contractual requirements or behavior codes;
- Establishing the audit feasibility – the most important factor is availability regarding: information and their opportunity, auditee's cooperation, time and resources;
- Audit team selection – it is made taking into account the professional competence; the size and members of the audit team are established depending on some factors of professional competence, audit type, legal requirements, communication; to assure the global professional competence, the below steps are followed:
  - Identifying the knowledge and skills necessary to get to audit purposes;

- Selection of audit team members in such way to cover all knowledge and necessary skills;

If some knowledge and skills are not covered by audit team then technical experts are included in it. Also, audit beginners can be included into audit team, but they must not audit guidance.

- Establishing the initial contact with auditee – it is made by persons responsible for audit program management or the audit team leader; the goal of the initial contact is for communication, authority regulation, information exchange, rule establishing, third party participation.

The stage for document analysis includes activities for audit evidence gathering from auditee's documents in relation to audit criteria. Documentation includes official papers and previous audit reports. Sometimes, this activity is made after the beginning of the audit to the site. The audit process can be stopped or suspended whether the auditee's documents are inadequate in relation to the audit purpose.

The third stage of the audit process is preparing the audit activities on site. The stage includes activities regarding (ISO 19011, 2003):

- Preparing the audit plan – it is made by audit team leader to assure the basis of understanding among audit client, audit team and auditee;
- Assigning activities among audit team members – it is made by audit team leader in accordance to professional competence, skills and independence of the auditors, efficacy use of the resources, technical experts and audit beginners; there can be made changes during the audit process to assure the accomplishment of the audit purposes;
- Document preparing – audit team members analyze the relevant information and prepare the work documents; the documents list include:
  - Check lists and sampling plans;
  - Forms for information recording: audit evidences, observations and records of the meeting.

The stage for carrying out the audit activities on site takes into account the following activities (ISO 19011, 2003):

- Carrying out the opening meeting – opening meeting is hold together with auditee's management to approve the audit plan and other details regarding the audit organization;
- Communication during the audit – it is necessary to made some conventions regarding communication with auditee and within audit team; audit team leader must periodically communicate the audit stage, problems with auditee and audit client, audit evidence with high risk, any issue out of the audit scope, audit evidences that proof the purposes are unreachable;
- Roles and responsibilities of the guides and observers – guides and observers accompany the audit team, but they are not member of this one; they acts to the request of audit team leader;
- Information gathering and their check – during the audit process, relevant information is gathered and checked; only verified information can be audit evidence; audit evidences are recorded and they are based on information samples; gathering process of the information during the audit until audit conclusions includes the following activities:

- Information collecting from information sources through sampling and their check; checked information can be concretized into audit evidence;
- Audit evidences are assessed in relation to audit criteria; it can be obtained audit observations;
- Audit observations are analyzed to state the audit conclusions;

The gathering methods of the information are:

- Interviews;
- Observation of the activities;
- Analysis of the documents;

- Generation of the audit observations – audit evidences are assessed in relation to audit criteria to generate audit observations; audit observations indicate compliance or noncompliance to audit criteria; audit evidences that sustain a noncompliance conclusion must be clear and recorded;
- Preparing the audit conclusions – audit team must consider the following issues:
  - Analysis of the audit observations in relation to audit purposes;
  - Agreement on audit conclusions;
  - Recommendation preparing;
  - Discussion on follow-up activity;
- Carrying out the closing meeting – closing meeting is coordinated by audit team leader and it is hold to present the audit observations and conclusions to be understand and agree by auditee; divergent opinions regarding the audit observations and conclusions must be discussed; also, it can be establish a deadline for auditee to present a plan for corrective and preventive actions.

Preparation, approval and distribution of the audit report represent the next stage in carrying out an audit process. This stage includes the following activities (ISO 19011, 2003):

- Preparation of the audit report – audit team leader is responsible for preparation of the audit report; audit report has to be complete, exact, concise, clear and refers to the following elements:
- Approval and distribution of the audit report – audit report is dated, analyzed and approved in accordance to the specifications from audit program; it is property of the audit client and it is distributed to the receivers named by the audit client.

The audit process is closed when the activities included in audit plan are accomplished and the audit report was approved and distributed. Audit team members must respect confidentiality of the data recorded in audit documents in accordance with the regulations.

The follow-up audit contains activities that can be considered as part of audit process or not. The audit conclusions lead to the need for corrective, preventive or improvement actions. The auditee must implement these actions and they are reported to the audit client. A new audit process controls the efficacy of these actions.

The audit process stages described above can be applied to different levels of audit: management system, process, product or service. For instance, during development of the distributed informatics, systems the audit process has to consider many changes that appear during its execution. These changes aim: management team, new IT&C technologies, new management techniques, analysis and implementation team, economic environment.

In its fundamental meaning, the audit of the distributed informatics systems checks whether this system gets to purposes that it was developed for.

3. Support documents for informatics audit process

A document represents any kind of support used to depict information by means of symbolic marks.

Depending on their use purpose, the support documents for informatics audit process are classified in the below classes:

- Official documents – they are documents use as reference points for audit process; in this class, the following documents are included: standards, guidelines, procedure, laws, regulations and so forth; these documents are elaborated by professional associations or government institutions;
- Internal documents of the organization – they are documents use to implement the management strategies of the organization; some of these documents are results of the legal requirements regarding the business: financial, accounting and so forth; other documents are used only within organization: databases, performance reports, feedback from the clients and so forth; for instance, previous audit reports are documents for internal use and this document can be use as initial point in a new audit process;
- Documents for internal use of the audit process – they are documents elaborated in audit processes; these documents are generated and filled in by audit team members to record information, audit evidences, audit observations, conclusions and so forth.

The audit program is a document used to organize audit processes. The records of the audit program are (ISO 19011, 2003):

- Audit plans;
- Audit reports;
- Noncompliance reports;
- Reports for corrective and preventive actions;
- Follow-up activities reports;
- Results of audit program analysis;
- Reports regarding the audit team members: assessment of auditors' competence and performance, selection of the audit team and competence maintenance and improvement.

Documents used for audit records must be safely stored to be easily found and readable. Also, these documents must meet the integrity characteristic to conclude correct and objective opinions regarding the audit object.

The audit plan includes the following elements (ISO 19011, 2003):

- Audit purposes;
- Audit criteria and reference documents;
- Audit scope;
- Date and locations where audit activities will be done;
- Period of time and duration to carry out audit activities on site;
- Audit team members' roles and responsibilities;

- Resource allocation for critical audit zones;
- Establishing the auditee's representative;
- Work language;
- Elements of the audit report;
- Logistics;
- Confidentiality issues;
- Follow-up activities of the audit;

The audit report is a complete, exact, concise and clear record which concludes the audit process. An audit process has to contain the following elements (ISO 19011, 2003):

- Audit purposes;
- Audit scope;
- Audit client;
- Audit team leader and members;
- Dates and places where the audit activities was carried out on site;
- Audit criteria;
- Audit observations;
- Audit conclusions.

Also, the audit report can contain or refer to the following elements:

- Audit plan;
- Auditee's representatives;
- Audit summary, highlighting the factors that decrease the confidence in audit conclusions;
- Uncovered areas, although they were included into audit scope;
- Confirmation for audit purpose accomplishment within the audit scope in accordance to audit plan;
- Unresolved divergent opinions;
- Recommendations for improvement whether they were specified in audit purposes;
- Follow-up action plan;
- Statement of audit report confidentiality;
- Distribution list of the audit report.

The audit report is elaborated by auditors with a high level of competence and experience in the audit field. When an opposite opinion is expressed, the audit report must present the causes of that opinion in a clear and documented way.

In audit report elaboration process, the auditor must have an independent position and has to be out of conflicts of interests, regardless of the beneficiary or the destination of the audit reports.

The quality of an audit report is determined by the professional competence and skills of the auditors. A certified auditor confers value to the audit report. Auditors are responsible whether the audit report is or not ready to the established deadline.

During the audit process, background documentation is necessary to establish the elements that highlight concordance between audit activities and standards applied in audited field. The worksheet is the main support for audit report and review of whole activity (Sergiu Capisizu, 2006).

4. Conclusions

The distributed informatics systems became very popular for the most part of the organizations and government departments due to evolution of the IT&C technologies and business globalization.

The audit processes are lead by persons with high level of professional competencies and skills. They follow the standards, guidelines, procedures and legal requirements to assess distributed informatics systems. Standards impose a rigorous way to organize and carry out the audit processes on stages with precise delimitations between audit stages.

Audit processes are parts of the audit program as an organizational strategy to assess the quality of the distributed informatics systems.

Audit processes are documented, each audit stage being accompanied by papers to get to conclusions based on audit evidences.

References

1. Baicu, F. and Baicu, A. M. **Auditul si securitatea sistemelor informatice,** Victor Printing House, Bucharest, 2003
2. Popa, M. **Detection of the Security Vulnerabilities in Web Applications**, Informatica Economica, 1(49), 2009, pp. 127–136
3. Popa, M. and Paraschiv, A. **Premises for Development of an Assessment System for Security Audit of Distributed Information System**, in „Proceedings of the Ninth International Conference on Informatics in Economy – Section 7: Informatics Security", May 7 – 8, 2009, ASE Bucharest, pp. 827 – 832
4. Ivan, I., Nosca, G. and Capisizu, S. **Auditul sistemelor informatice,** ASE Printing House, Bucharest, 2005
5. Capisizu, S. **Models and Techniques for Development the Economic Information Audit**, PhD Thesis, ASE Bucharest, 2006
6. Popa, M., Toma, C. and Amancei, C. **Characteristics of the audit Processes for Distributed Informatics Systems,** Informatica Economica, 3(49), 2009, (paper submitted to be published)
7. Popa, M., Florescu, M. and Bodea, C. **Information System Quality Evaluation Based on Audit Processes,** in „Proceedings of the 2008 International Conference of Information Engineering", (International Association of Engineers, Imperial College London), July 2 – 4, 2008, pp. 494 – 496
8. Popa, M., Alecu, F. and Amancei, C. **Characteristics of the Audit Process for Information Systems,** in "Proceedings of the International Conference Competitiveness and European Integration – Business Information Systems & Collaborative Support Systems in Business", UBB Cluj-Napoca, October 26 – 27, 2007, pp. 295 – 299
9. * * * **Ghid pentru auditarea sistemelor de management al calitatii si/sau de mediu**, ASRO, SR EN ISO 190011, July 2003

[1] 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.

[2]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 as teaching

assistant in 2002. He has been university lecturer since 2006. Currently, he is university 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. Between 2003 and 2008 he was a member of the editorial team for the journal Economic Computation and Economic Cybernetics Studies and Research.

He was involved as project manager or research team member in research projects on following topics: virtual intelligent manufacturing processes, developing and testing an automated system of risk analysis, diagnosis and decision to support the medical act, system of quality assessment services generated by mobile applications in electronic business, system of quality assessment for on-line public services for citizens and businesses, system of indicators for evaluating IT project management, collaborative informatics systems in the global economy, methodology of applications development for managing the IT project portfolios, evaluation system of the entities based on text, models to estimate the cost of e-business applications, model base for software quality management, designing and implementing the virtual enterprise and platform for estimating costs of testing object oriented software prototypes.

Currently, he is involved as project manager in a research project on topic Implementation of the Quantitative Methods in Distributed Informatics System Audit and as research team member in techniques for classification and recognition with applications in identification documents similarity.

He is certified as project manager IPMA Level D, Certified Project Management Associate. Also, he holds more awards and diplomas for his research activity.

His interest fields are: software engineering, informatics security, software development, project management, informatics audit, data and software quality.

He is member of Research Center of Excellence (ECO-INFOSOC), Association for Promoting the Higher Education in Computer Science in Economics (INFOREC) and Association for Development through Science and Education (ADSE).

List of Main Publications (2005 - 2009)

Ion IVAN, Marius POPA and Paul POCATILU (coordinators) **Structuri de date,** Bucharest: ASE Printing House, 2008, vol. I Tipologii de structuri de date; vol. II Managementul structurilor de date

Marius POPA **Evaluarea calitatii entitatilor text – Teorie si practica,** Bucharest: ASE Printing House, 2005

Marius POPA **Detection of the Security Vulnerabilities in Web Applications,** Informatica Economica, vol. 13, no. 1(49), 2009, pp. 127 – 136

Cristian TOMA, Marius POPA, Catalin BOJA and Miruna VASILACHE **Secure Electronic Cards in Public Services,** Informatica Economica, vol. 12, no. 2(46), 2008, pp. 80 – 85

Cristian TOMA, Marius POPA and Catalin BOJA **Smart Card Based Solution for Non-Repudiation in GSM WAP Applications,** WSEAS Transactions on Computers, vol. 7, Issue 5, May 2008, pp. 453 – 462

Ion IVAN, Dragos ANASTASIU, Catalin BOJA, Marius POPA and Cristian TOMA **Structures Text Entities Dependecy Graph Building - Theory and Practice,** WSEAS Transactions on Computers, vol. 6, Issue 5, May 2007, pp. 835 – 842

Ion IVAN, Cristian TOMA, Marius POPA and Catalin BOJA **Secure Platform for Digital Rights Management Distribution,** WSEAS Transactions on Computers, vol. 6, Issue 3, March 2007, pp. 478 – 485

[3]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 gratuated from the BRIE master program in 2005 and PhD. Stage in 2008. In present, he is universitary lecturer at Economic Informatics Department and he is member in research structures such as ECO-INFOSOC, recognized by CNCSIS in 2005 as excellence center, since 2004 – involved 2 major CEEX research projects. Also, he is member of professional association INFOREC România since 2008.

Since the begining – 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 comitee. In 2008, he was initiator and member of the organization team for the International Conference on Security for Information Technology and Communication, SECITC 2008, edition 2008, www.secitc.eu.

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 assembly language, 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 procedings.

The most recent book: Cristian TOMA – Security in Software Distributed Platforms, AES Publishing House, Bucharest 2008, presents development phases for various software architectures, platforms, components and protocols used in IT&C security field. The book combines at theoretical and practical level concepts from the mobile applications, smart-cards, computer netoworks and computational cryptography areas.

The content of the lectures and seminars are published also in electronic format on the web portal www.acs.ase.ro.

List of Main Publications (2005 - 2009)

Cristian TOMA, Catalin BOJA and Marius POPA **Solution for Non-Repudiation in GSM WAP Applications,** The 7th WSEAS International Conference on SOFTWARE ENGINEERING, PARALLEL and DISTRIBUTED SYSTEMS (SEPADS '08), Advances on Software Engineering, Parallel and Distributed Systems, University of Cambridge, UK, February 20-22, 2008, pp. 212 - 219

Cristian TOMA, Marius POPA, Catalin BOJA and Miruna VASILACHE **Secure Mobile Electronic Card Used in Medical Services, Applied Computing Conference,** Istanbul, Turkey, 27 - 30 May 2008, "Proceedings of the Applied Computing Conference , Computational Methods and Applied Computing", 2008, pp. 124 - 130

Ion IVAN, Cristian TOMA, Marius POPA and Catalin BOJA **Secure Platform for Digital Rights Management Distribution,** WSEAS Transactions on Computers, Issue 3, Volume 6, March 2007, pp. 478 – 485

Cristian TOMA **Secure Architecture for E-Money Transfer – SA4EMT**, SECITC 08 - The 1st International Conference on Security for Information Technology and Communication, JITCS - Journal of Information Technology and Communication Security, pp. 41-51

Cristian TOMA and Mihai DOINEA **Secure Mobile Architecture for E-Signature of Documents – SMA4ESD,** SECITC 08 - The 1st International Conference on Security for Information Technology and Communication, JITCS - Journal of Information Technology and Communication Security, pp. 101-109

Cristian TOMA and Catalin BOJA **Mobile Application Security Frameworks,** SECITC 08 - The 1st International Conference on Security for Information Technology and Communication, JITCS - Journal of Information Technology and Communication Security, pp. 109-121