

Information System Quality Evaluation Based on Audit Processes

M. Popa, M. Florescu, and C. Bodea

Abstract—The paper investigates how the quality of the information systems implemented in companies and other organizations can be improved after developing audit processes. The investigation is based on the standards elaborated for information system audit by standardization organizations. The paper highlights the framework, characteristics and the audit activities related to the quality of the information systems. Also, some methods and techniques used for auditing information systems included in the main IT audit standards are presented.

Index Terms— audit process, information system, quality.

I. INFORMATION 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, as in [14].

A system can be defined by the following elements:

- inputs;
- outputs;
- transformation process;
- system structure and its state.

A complex economic system is made by the following components, figure 1, [14]:

- decision system;
- operating system;
- information system.

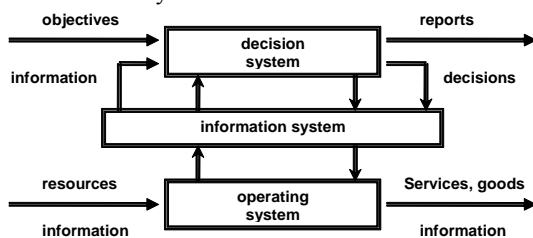


Figure 1 – The components of an economic system

Manuscript received March 5, 2008. This work was supported in part by the Romanian Ministry of Education and Research under Grant CEEEX 92/2006.

M. Popa is with the Computer Science in Economics Department, Academy of Economic Studies, Bucharest, Romania (phone: 0040-21-3191900.; fax: 0040-21-3191899; e-mail: marius.popa@ase.ro).

M. Florescu is with the Management Department, Faculty of Management, Academy of Economic Studies, Bucharest, Romania (e-mail: icefaceus@yahoo.com).

C. Bodea is with the Computer Science in Economics Department, Academy of Economic Studies, Bucharest, Romania (e-mail: bodea@ase.ro).

The *information system* resides in all the informational flows and circuits and all the methods, techniques used to process the data needed by the decision system.

The *information technology system* is a component of the information system that is in charge with collecting, processing, transmitting, storing and presenting the data by using computing systems. In other words, it is responsible for automatic processing of the data by using various methods and techniques.

The automatic data processing covers the collecting, transmitting, processing and storing operations, as in [14]:

- *collecting data* – takes place at the location where the primary data are generated;
- *processing data* – the primary data are transformed into final results;
- *transmitting data* – from the primary locations to the automatic processing systems;
- *storing data* – is responsible for data archiving on specific medium.

An information system has the following characteristics:

- collection of components;
- functional inter-correlation;
- data automatic processing;
- includes the following kinds of components: hardware, software, communications, users, organizational framework.

The information systems must be developed in accordance with the all informational flows and circuits and the needs of the decision system. Its quality evaluation can be made for the systems that are in use or for the systems that are in development stage. The results of the audit process development must be analyzed, and the conclusions must be translated into the procedures and actions implemented in the audited information system.

II. METHODS AND TECHNIQUES OF AUDIT FOR INFORMATION SYSTEM EVALUATION

The *audit* is the process through which the competent and independent persons collect and evaluates proofs to fundament an opinion regarding the correspondence degree among the observed things and some pre-established criteria, as in [8].

Through audit it is certified the correspondence degree between the reality and defined criteria. The results are reported to interested users. The goal is to increase the quality level through improvement of actions and indicators calculated for the traced quality characteristics.

The associations between objectives of quality and the developed processes to achieve them are highlighted in the below figure, as in [8].

Table no. 1 Association objectives – inserted processes

Objective	Main processes included
Evaluation	Management inspection, Technical inspection
Verification	Inspection, Examination
Validation	Testing
Conformity, Confirmation	Audit

In software production, it is pursued the un-biased evaluation of products and processes and the conformity with standards, specifications and procedures.

The audit has as main purposes the following:

- Initial point for development;
- Compliance or non-compliance with the designed specifications;
- Efficiency;
- Improvement;
- Prevention, correction and following-up.

Information systems are complex constructions designed and implemented for assisting in the activities developed in organizations.

The auditors must have expertise and they must develop audit processes in the following fields:

- Informatics systems;
- Software products;
- Data.

The information system audit analyzes the systems and the networks with the view of measuring the efficiency of technical and procedural control in order to minimize the risks. The informatics system auditing supposes discussions with the employees that establish the specifications, develop, test, lead, manage and use the computation systems [4].

For instance, there are many investigation techniques that use the following kinds of questions:

- Open questions: Who? What? Where? Why? When?;
- Close questions: Yes/No answers;
- Oriented questions: Don't you think ...?;
- Opinion questions: What is your opinion ...?;
- Investigation questions: Did you make ...?;
- Non-verbal questions: body language.

The software tools implemented in the informational systems of the organizations can reveal to the IT auditors the functionality of the software modules. Thus, the software tools are adjusted to be in conformance with the initial parameters or all module software is modified to respond to new requirements of the informational system. This kind of audit is real-time and is called continuous audit. The continuous audit addresses all the components of the information system, not only the IT component.

For instance, an extension language of XML called Extensible Business Reporting Language (XBRL) is used in order to provide continuous financial reporting which can lead to a real-time reporting for financial reports, as in [11].

There are many software tools for testing the security of the banking information system, such as:

- Vulnerability scanners;
- Network protocol analyzers;

- Intrusion detection systems;
- Wireless sniffers;
- Web scanners;
- E-mail server scanner;
- Software tools for interpretation of the questionnaire answers.

The information system quality level is assured by applying risk control strategies:

- Risk prevention;
- Risk impact reduction;
- Probability reduction of risk occurrence;
- Early detection of risks;
- Disaster recovery;
- Risk transfer.

The information system audit is a management tool for monitoring and verifying the quality characteristics level.

III. STANDARDIZATION OF THE AUDIT PROCESS

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 how these are accomplished.

The specialized character of the informatics systems audit and the skills needed to carry out such audits require standards applied on informatics system audit. The framework for the IS Auditing Standards provides multiple levels of guidance, as in [5]:

- 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 informatics system auditing standards; the auditor should consider the guidelines in order to determine how to achieve the 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.

In the international standard SR EN ISO 9001:2001 requirements for quality management system are contained, and the standard ISO 19011:2002 contains directions regarding auditing and auditors' qualification. The auditor is placed in interface between quality management and auditing process. The auditor has the task to respect the principles regarding quality management system, as in [8].

The information audit permits drawing a conclusion

statement regarding the efficient implementation of the quality management principles, depending on the quality level of the systems in use. In standard ISO 19011:2002, are presented the auditing principles that refer to the auditors and auditing processes. The principles that regard the auditors are, as it is shown in [8]:

- ethical behavior – represents the base of professionalism for the person who develops auditing processes;
- correct presentation – aims at the reporting of reality with maximum accuracy, evenly;
- professional responsibility – refers to perseverance in applying and the judgment used in auditing.

The standard BS7799 has been used since 1995 in Europe. It was adopted as international standard under the name ISO 17799. The standard has known successive improvements, the latest version being adopted in 2005. The ISO 17799:2005 standard structure contains 11 security controls regarding the information systems, as in [12], [16]:

1. Security Policy (1);
2. Organizing Information Security (2);
3. Asset Management (2);
4. Human Resources Security (3);
5. Physical and Environmental Security (2);
6. Communications and Operations Management (10);
7. Access Control (7);
8. Information Systems Acquisition, Development and Maintenance (6);
9. Information Security Incident Management (2);
10. Business Continuity Management (1);
11. Compliance (3).

The audit process is developed in accordance with the audit program.

A very important component of the information system audit is the security controls. For this component, the employees are the central piece in order to protect and keep the information system within the designed parameters.

IV. CONCLUSION

The audit of information systems permits their quality level evaluation. The evaluation is made by human subjects who must be independent and have a very good professional background and skills in order to lead the audit process.

The audit results must correct some aspects concerning the information systems development and completion. Hence, many aspects regarding the developed activities during information system life cycle can be improved through audit processes. In order to achieve that goal, there were elaborated standards by international standardization organizations with the view of establishing the working procedures regarding the techniques and methods used in the evaluation activities.

REFERENCES

- [1] A. D. Chambers, J. M. Court, *Computer Auditing*, Pittman Publishing, London, UK, 1991
- [2] S. Capisizu, G. Noșca, M. Popa, "Informatics Audit", The symposium with international participation „The 37th International Scientific

- Symposium of METRA”, Bucharest, May 25-26, 2006, The 37th International Scientific Symposium of METRA, Bucharest, 2006
- [3] I. Douglas, *Computer Audit & Control Handbook*, Butterworth and Heinemann, Oxford, UK, 1995
- [4] G. Hinson, *Frequently Avoided Questions about computer auditing*, <http://www.isect.com>
- [5] Information Systems Audit and Control Association, *IS Standards, Guidelines and Procedures for Auditing and Control Professionals*, 7th of September, 2006
- [6] I. Ivan, G. Noșca, S. Capisizu, *Auditul Sistemelor Informaticice*, ASE Printing House, 2005
- [7] S. Buchanan, F. Gibb, "The information audit: an integrated strategic approach", in *International Journal of Information Management*, 18(1), pp. 29-47
- [8] I. Ivan, M. Popa, S. Capisizu, "Quality Management through Informatics Audit", in *Proceedings of the 6th International Economic Symposium*, Transilvania University of Brașov, May 19-20, 2006
- [9] I. Ivan, P. Pocatilu, T. Mihai, C. Stanca, "Data Certification", in *Proceeding of the 2000 MIT Conference on Information Quality*, Cambridge, Massachusetts, USA
- [10] J. Kramer, *The CISA Prep Guide: Mastering the Certified Information Systems Auditor Exam*, Wiley Publishing Inc., 2003
- [11] S. Flowerday, R. von Solms, "Continuous Auditing: Verifying Information Integrity and Providing Assurances for Financial Reports", *Computer Fraud & Security*, vol. 2005, Issue 7, July 2005, pp. 12 – 16
- [12] M. Popa, M. Doinea, "Audit Characteristics for Information System Security", in *The Proceedings of the Eight International Conference on Informatics in Economy*, Academy of Economic Studies of Bucharest, May 17-18, 2007, pp. 938 – 943
- [13] M. Popa, F. Alecu, "ERP Informatics System Audit", *International Conference „Knowledge Management – Projects, Systems and Technologies”*, vol. II „Reinforcement and Extension of Universities & Business Community Partnerships in the Knowledge Era”, November 9 – 10, 2006, pp. 109 – 116
- [14] M. Popa, F. Alecu, C. Amancei, „Characteristics of the Audit Process for Information Systems”, in *he Proceedings of the International Conference Competitiveness and European Integration – Business Information Systems & Collaborative Support Systems in Business*, 2007, Editura Risoprint, Cluj-Napoca, pp. 295 – 299
- [15] International Standard ISO/IEC 27001, *Information Technology, Security Techniques, Information Security Management Systems, Requirements*, 2005
- [16] M. Florescu, D Hincu, "Increase of economic Competitiveness. Analysis of the current situation" in *the Proceedings of the Conference „Fondurile structurale și de coeziune ca premisă a dezvoltării mediului de afaceri din România”*, ISBN 978-973-749-204-3
- [17] M. Florescu, *Dissertation: Theories of Entrepreneurship Teaching Quantitative Materials with Cases, How Business Schools Lost Their Way Education for Judgment*, European Foundation for Entrepreneurship Research A Framework for Course and Intellectual Development HARVARD BUSINESS SCHOOL – USA
- [18] International Standard ISO/IEC 17799, *Information Technology, Security Techniques, Code of Practice for Information Security Management, Second Edition*, 2005