The Major IT Audit Concerns inside the Information System Analyze and Design

Surcel Traian

Academy of Economic Studies

tsurcel@ase.ro

Alecu Felician

Academy of Economic Studies

alecu.felician@ie.ase.ro

Abstract

The IT Audit is an important request for the Information System quality certification regarding: compliance, credibility, performance and security. The Information System Analyze and Design Methodologies, starting with SSADM thru EISADM, are not close up with the rapid progress made by the audit activities. The methodologies must be improved in order to create the theoretical framework to guide the IT systems developers identifying and analyzing the vulnerabilities, threatens and risks evaluation, so, they can define and implement the general and applications control procedures. The procedures will be the milestones for the IT Audit Management. Inside the Information System Analyze and Design Methodology. The methodology specifications need to contain a special section for developing the IT Security Policy from where must not be missing the Business Continuity and Disaster Recovery Plan.

Keywords: *IT Governance, IT Audit, Information System Analyze and Design, Audit Controls and Procedures, IT Security Policy*

IT governance and audit

IT governance is the concept that defines the current processes of all IT resources of the organization: information, IT&C infrastructure, IT processes and human resources [5].

IT governance objectives are related to the integration and institutionalization of best practices that provide more than a processing performance of information through computer systems.

IT governance ensures the alignment of IT strategy with the objectives of undertaking economic activities by linking IT activities with the business processes, ensures the

management of the IT investments, information resources and last but not least ensures proper management of IT risks. Like any management system, the IT governance is using the assessment-control for a proper base of operational decisions on the conduct of IT processes or objectives, if they were not sensibly established.

The internal control introduced by this feature is intended to prevent the creation of IT system failures, to signal the errors caused by "something should go wrong and go wrong or has gone bad" (What Could Go Wrong).

These failures represent risks that have consequences as material losses, financial or image. Internal controls are defined by the design of the system. But, are there sufficient controls established, are the correct control procedures applied, are the appropriate measures taken? The answer to these problems is given by the IT audit.

The IT audit is the final certification degree of credibility of an IT system, of the correctness of the results and of the completeness of processing, certifying compliance with laws and standards, certifying the system is functioning safely and security.

A large part of the nonconformity regarding the implementation and quality control procedures outlined by the IT audit is determined by the design and implementation errors. The usual methodologies do not contain a coherent set of explicit rules to guide even require systems designers to define and implement control procedures in accordance with the requirements of future audits.

Methodologies dealing with priority the issues of validation and control that are incorporated into the structure of the application programs, especially programs used to update access and query the databases [3]. But general controls and application controls, used by the most important IT audit standards, for example provided by ISACA COBIT, or ISA supplied by IFAC, are more numerous and complex.

Therefore, we appreciate that the information systems methodologies of analysis and design must be updated in order to follow the audit methodologies trends.

An analytical approach of audit controls

The standards of audit are dividing the controls into two main categories: general controls and application controls.

The general controls class relates to controls regarding the lifecycle of the IT system, the planning and organization of the system, to controls related to the management of changes and not least the IT security controls and ensures business continuity recovery in the event of disasters. At the level of detail, the auditor must check the system documentation and the real implementation in order to see if they comply with requirements concerning the following:

- development and approval of IT strategies;
- contract basis for the system implementation;
- budget and budget implementation plan according to the calendar;
- choosing and contracting the hardware configuration and software licenses, the training applications to be used for the staff;

- setup the organizational scheme, establish the levels of skills, duties and responsibilities of the jobs;
- development and implementation of security policies that must include business continuity plan and recovery in the case of disasters.

The application controls class takes us closer to the concrete design of the basic components of the system: forms, documents, reports, files, database, software, and interfaces with users.

We propose a separation of application controls in two categories. Given the orientation of the checks, the two categories are:

- technical controls;
- IT environment controls.

Technical controls are aiming the proper functioning of the programs and modules Informatics. This proper functioning is assured by the following:

- validate the data entry (format, range, checksum), the reports (logical correlation between the columns, key checking), the algorithms (set of test data), etc.
- the sequence the processing logic that prevents the duplication of updates and allows the compliance with the databases integrity requirements.

As we can easily notice, this type of control is found in the algorithms of the programs, automatically executed when running various software modules.

IT environment controls are aiming the procedures, manuals or semiautomatic, that articulates IT system with the information system of economic organization. In these control procedures, the human factor is very important and this is one of the vulnerabilities coming from the superficiality of compliance with the documentation. Here are a few of these controls:

- first of all, the existence of a classification of information and tables with the owners of information for prioritizing security information;
- authorization of procedures for entering of data, or dissemination of reports; updating the permanent data from the database;
- the existence of procedures for archiving electronic information entered into the system without having a correspondent in a primary document;
- the existence of test data and results of testing programs and modules;
- the control of customization of ERP system implementations;
- the existence and implementation of procedures to control the exchange of data with additional external systems other than automatic ones;
- the control of change management and separation of responsibilities;

We believe that this distinction between the two categories of application controls is useful to guide the efforts of system designers because:

- technical controls are mostly known, inventoried and classified in methodology standards, such as Romanian standard SR ISO / IEC 17799 - 2004 "Information Technology - code of good practice for information security management". They are mainly implemented by programs.
- computerized environmental controls are bearing the print of the particular business processes and management that interferes in the area of IT&C. They should be projected and designed by the team of system analysts.

The need of a methodological framework appropriate for the design and implementation of these controls is clearly a certainty in the conditions when the audit systems becomes an imperative requirement in order to meet the expectations of the IT&C users.

Audit tracers of the methodology used to design the IT

ERP implementation fever, the use of the object oriented technology, the UML diagrams, the CASE tools, which aims to reach an efficient design of information systems have resulted, into the methodologies used by analysts, to an increase of the technical application controls. Therefore we recommend, starting with the analysis phase, the need for another phase of analysis to include a series of phases and activities related to future audit processes.

In the phase of the analysis of the existing system, we must find a stage for inventory and analysis of vulnerabilities, threats and risks to which the IT system may be exposed. Such a review should be implemented in a group of lists on this subject. Based on these lists it is possible to develop further analysis of relevant cost of reduction and prevention of loss in order to establish priorities and controls to be implemented.

During the design phase, for each stage, we have: designing forms and formats for data input, for reports, database design, design of the programs, interfaces. To follow the sequence reviewed by D. Oprea [5], we should include activities for defining procedures of the environment and technical control.

The design stage of the inputs must provide at least three control procedures:

- procedure for approving the input of the data, IADP - Input Data Authoring Procedure;
- procedure for solving the errors regarding the logical checking of the data, DECP - Data Error Check Procedure;
- procedure for archiving electronic information entered without a correspondent in a primary document, EIWD - Electronic Information Without primaryDocument.

The IADP procedure does not refer only to validate the access rights but also it concerns the authorization of input data sets in terms of authentication the data source and the position regarding the management and reporting elements and so on.

The output and reports design stage should include:

- the procedure responsible to assure the security of the reports on the routes of distribution, other than electronic ones, RDSF - Report Distribution Security Flow;
- procedure for authentication the rights regarding the printing and archiving of outdated reports, RPAP - Report Printing and Archives Procedure;

The program design stage includes many procedures but we will stop at just a few more relevant for the certification of accuracy, completeness and computations:

- the RT procedure - Run Twice, applies unannounced, is intended to verify that running twice the same procedure on the same set of data we obtain the same results;
- the FRUK procedure - Freeze Update and Check, applies in the case when we can "stop" for a short time the access to any data in order to operate a predefined set of updates to the database, followed by comparing the results with the manually estimated ones;
- the CMP procedure - Change Control Management, which involves the entire flow of operations, from the change requests in hardware or software to the implementation of the new software versions, hardware configurations or database levels.

A special mention should be made in relation to the objective need of defining the methodological handbook for the document named "Security Policy" of organization data starting from the current standards. Because we cannot discuss about the security of the IT systems without taking into consideration the recovery plan in case of disaster, DRP - Disaster Recovery Plan, it is necessary to design a procedure of „cloning the IT system". Through this complex procedure we obtain a mirror copy of the real system, which can run in parallel or can be quickly turned on and to replace the damaged system.

All these procedures must be documented, both through on-line tutorials and documentation in the classical form that comes together with any system.

Conclusions

The audit of the IT systems is a process that chronologically comes "after" the period in which the system was designed and implemented. It represents a critical point of view regarding the finished product. Like any constructive criticism, the audit is necessary and welcome, but corrections to be made as a result of non-conformities reported by the audit team involves additional costs that are sometimes difficult to implement, time consuming, produces a discomfort to the users that must also acquire the new changes. Some of these shortcomings are determined by the fact we are coming from the audit to the IT system. We can proceed in a reversed way, foreseeing from the very beginning, by the methodology of design information,

systems auditing controls that we have analyzed, which, once implemented, to be monitored by IT management. We can even talk of IT management audit as a component of the management department, IT division or even as a new role, the IT audit manager.

Thus, we have created the preconditions for a faster and more realistic certification, by using the audit of the quality, security and safety operation of a system.

References

[1] Kenneth C. Laudon, Jane P. Laudon, „*Essential for Management Information System*" , Editura Prentice Hall, 2002

[2î Mitchel H. Levine, „*Performing an Audit of an Automated Mainframe Software Change Management System*, http://www.autoserve.com/articles/art_36.htm, 2008

[3] Oprea D., Dumitru F, Meşniţă G, „*Proiectarea sistemelor informationale*", Editura Universităţii „Alexandru Ioan Cuza", 2006

[4] Traian Surcel, „*Auditul şi managementul sistemelor informatice*", the Proceedings of the 2006 International Conference on Comerce", ASE, 2006

[5] Surcel T, Mârşanu R, Reveiu A., Pocatilu P., Felicia A., Bologa R, *„Informatică Economică"*, Editura Tribuna Eonomică, 2004

[6] IT Governance Institute „*Control Objectives for Information and related Technology*", v4.1 2007

[7] Ion Ivan, Alecu Felician, Sergiu Capisizu, *Auditul Informatic*, Economistul, 2005

Integrarea problemelor majore de audit in metodologia de analiză si proiectare a sistemelor informatice

Auditul IT este o cerin□ă importantă pentru certificarea calităţii sistemelor informa□ionale privind aspecte legate de standarde, credibilitate, performanţă şi securitate. Analiza sistemului informa□ional şi metodologiile de elaborare, incepand cu SSADM prin EISADM, nu □in pasul cu progresul rapid înregistrat de către activităţile de audit. Aceste metodologii trebuie să fie îmbunătăţite în scopul de a crea un cadru teoretic necesar pentru a ghida dezvoltatorii de sisteme IT în identificarea si analiza zonelor vulnerabile, ameninţărilor şi evaluarea riscurilor, astfel încât să aibă posibilitatea de a defini şi implementa proceduri de control generale şi de aplicaţii. Aceste proceduri vor fi pietre de hotar pentru audit de management IT. Specifica□iile metdologiei trebuie să conţină o secţiune specială legată de dezvoltarea Politicii de Securitate IT din care nu trebuie să lipsească planurile de continuitate a afacerii şi de recuperare în caz de avarie.