IMPROVING THE QUALITY OF THE INFORMATION PRESENTED IN FINANCIAL STATEMENTS BY USING INFORMATION TECHNOLOGY

VASILE DUMITRAŞ [*]

ABSTRACT: *Information technology can contribute significantly to business efficiency, including also enterprise governance, through appropriate and effective use. In most cases, it is difficult to determine which technologies are relevant to business needs and the use of appropriate options is not always clear. The development of information society, characterized by integration and automatization of processes and controls, by increased operational security of systems but also increasing dependence on them, and accompanied also by increased requirements of correct and operative information creates the need for new approaches of procedures and financial systems architectures.*

KEY WORDS: *information technology; financial accounting systems; application controls; estimating the risk; typical abnormalities in operating the computer system.*

JEL CLASSIFICATION: *M40; M42; M48.*

1. INTRODUCTION

The complexity of the information system is provided by a number of features relating to: *the volume of transactions*, *data validation procedures or data transfers between applications*, *automatic generation of transactions*, *communication with other applications or systems*, *complexity of calculation algorithms*, *use of information from external data sources*.

The increase in exchange of computerized data, the development of management facilities, the multiplication of electronic services, are issues that lead to the need of consumer confidence in information, as well as to the the need for systematic verification of the reality of information acquired. Production and communication of accounting information is a service which involves the concepts of *time* and *risk*.

[*] *Ph.D. Student,"Valahia" University of Târgovişte, Romania,* vasile.dumitras@yahoo.com

2. CHARACTERISTIC ASPECTS OF PROCESSING IN A COMPUTERIZED ENVIRONMENT

The smooth functioning of ***financial accounting systems*** must be ensured through specific IT procedures having the following specific aspects of processing in computerized environment:

a) The complexity of processing flows can generate lack of intermediate forms through which the transaction evolves, yielding in most cases only one final form and sometimes only available in electronic format or only for a short period of time. In the absence of appropriate validation procedures, errors may be difficult to detect by manual procedures.

b) Alteration of accounting information can be caused by the existence of systematic errors or anomalies in programs functioning that affect the processing of the entire amount of data and lead to erroneous results, difficult to correct by manual procedures, given the high volume of transactions and complexity of processing algorithms.

c) Concentration of operating procedures with incompatible functionality at the level of the same individual, which, according to the laws or internal regulations concerning the segregation of duties, should be operated by different people, generates the execution of incompatible functions and the possibility of altering the information content depending on personal interests. An important requirement related to the operation of computer applications is distributing the application throuought theentity and allocating access rights in accordance with the requirements for segregation of duties imposed by the law.

d) Due to human intervention, which is not always associated with strict protection regarding access authorization and intervention on data, in developing and maintaining the information system, there is a high potential for altering the data without explicit proof.

e) Following the automatic management of large volumes of data without human intervention, there is a risk of no timely detection of errors due to design faults or update of software packages.

f) In the case of procedures or transactions executed automatically, authorization by management may be implicit in the way the system was designed and developed for subsequent changes, which implies the absence of an authorization system similar to the manual system performed over procedures and transactions.

g) The effectiveness of the manual control procedures is affected by the effectiveness of IT procedures when the the manual procedures are based on documents and reports produced automatically by the computer system.

h) The extension of the internal control structure with specialized procedures based on the use of information technology has effects on the entity's activity monitoring plan through the use of analytical tools provided by the information system.

i) Performing tests on a large volume of data, by using computer assisted tools and techniques is facilitated by the existence of analysis and processing provided by the infromation system.

j) Risk assessment during audit missions in a computerized environment must consider the likelihood of obtaining false information with significant impact on the audit as a result of deficiencies in the information system functioning. These deficiencies can be related both to the quality of hardware and/or software infrastructure hardware, to software applications development and maintenance, to system operating and information system security, to the quality of the personnel involved in the information system functioning, to the quality of technical documentation, as well as to unauthorized interventions to applications, databases or procedural requirements imposed in the system.

3. THE LEGAL FRAMEWORK RELATED TO THE CRITERIA AND MINIMUM REQUIREMENTS REGARDING MANAGEMENT AND ACCOUNTING INFORMATION SYSTEMS

Most companies use software products for management and accounting. As a result of accounting information requirements by its users, the software products must meet, in turn, a number of specific requirements. There are many developments of such products in Romania and they must report to a number of criteria and minimum requirements, governed primarily by methodological norms of the Ministry of Finance taken by the Corps of Chartered Certified Accountants (CECCAR). These concern mainly the following aspects:

Internal control:

a) updates of the computer system in accordance with legislative changes;
b) knowledge of computer operation system by users (operating personnel);
c) access to data (privacy, use of passwords for access to data and system);
d) options for choosing the type of magnetic media for backup;
e) possibilities for detecting and resolving errors.

External control:

a) possibilities of complete or sample verification of the processing procedures ;
b) possibilities of complete or sample verification of the transactions recorded in accounting;
c) possibilities of complete or sample verification of the the processing flow by tests of control.

Minimum criteria:

a) compliance with the law;
b) specification of the type of support which ensures safe processing of information;
c) complete verification of each individual information recorded;

d) compliance of lists with the chronological criterion and impossibility of further update of the the list;
e) the automatic transferability of balances from the previous period as opening balances in the current period;
f) data retention (archiving) under the Accounting Law 82/1991;
g) the possibility of the restoration of archived data;
h) the impossibility of updating data from previous reporting periods;
i) to allow recording of essential information for identifying transactions: date, journal name, page number or registration number, document number;
j) access protected by passwords ;
k) identification in lists of the economic unity, the chronological pagination, document type, the reporting period, the date of listing and software version number;
l) to allow printing synthetic documents needed by the company's management;
m) to comply with the informational content for special forms;
n) to ensure consistency between the general ledger of each account and journal record;
o) to meet the requirements of database normalization in respect of the accounts and documents;
p) to provide the possibility of updating accounts without affecting the business management;
q) to have adequate technical documentation of software characteristics (mono / multi-post, single / multi company, file portability, network architecture, applications) in order to allow optimum utilization;
r) to determine the type of organization for data collection (batches with subsequent control, real time with immediate control, combined);
s) not to limit the amount of accounting information;
t) to ensure data security and reliability;
u) to provide updates of the procedures for processing financial and accounting information;
v) to ensure continuity in the event of closure of the software development activity, including archiving and restoring data;
w) to provide version management functionalities.

4. ANALYSIS OF THE RISKS INVOLVED IN THE USE OF ACCOUNTING INFORMATION SYSTEMS ON QUALITY OF INFORMATION PRESENTED IN FINANCIAL STATEMENTS

Auditing of accounting information when an information systems is used, is a process through which the following are aimed: to express an opinion on the correctness of financial statements, to determine the degree of honesty in reporting the financial statements, to identify fraud and errors. Also, the extension of audit missions, both as scope as well as complexity, requires emphasizing the need of performing them by using computers in a computerized environment.

For a financial management and accounting software, the control ssystem has the following levels:

- ***Examining the financial statements*** to determine whether the transactions accurately reflect the operations performed: correct recording in accounts of test transactions test, reflecting these transactions in accounting reports, respecting the formats required by law, etc.
- ***Output controls*** are designed to verify that the temporary files generated for printing (in spooler) before transmission to the printer can be altered without adequate protection, prior to being listed.
- ***Processing controls*** are implemented to verify the correct processing of exchange rates, fees, the application of overhead rates, the use of fares, etc.
- ***Input controls*** are designed to verify that the accounting documents refer to the relevant accounting period, that the chart of accounts is used correctly, that the application allows automated accounting equalities, etc.
- ***Preventing unauthorized acces to the system.***
- ***Ensure that the correct accounting software version is installed on the computers*** and not untested versions that may contain programming errors.
- ***Controls on the operating system*** provides verification that access to the financial management and accounting application is controlled and only authorized users operate it.
- ***Controls on access to the network*** ensure that unauthorized users can not access the systems within the network.
- ***Auditing security system of applications and Internet connections*** to verify the existence and functions of the security officer, as well as application level controls in order to identify risks and adopt measures to reduce them to acceptable levels.
- ***Selection and training of personnel*** provide assurance that selection and training procedures reduce the risk of human error.
- ***Physical and environmental controls***: ensure physical protection of computer systems.
- ***Management policies and standards*** cover all categories of controls across all levels.

Application controls are specific procedures to control applications, providing assurance that all transactions are authorized and recorded, processed completely, accurately and timely. Application controls consist of manual procedures performed by users (user controls) and automatic procedures or controls performed by the application. Application controls are specific for one application and may have a direct impact on individual transaction processing. They generally refer to those application embedded procedures to ensure that only valid transactions are processed and recorded completely and correctly in the application's files, as well as to manual procedures which operate in conjunction with the application.

The most common application controls are:

a) existence of procedures for automatic generation of output statements by the application;
b) existence of fucntionality for export of reports in electronic form within the system;
c) validity and consistency of data within the application's database;
d) existence of discontinuities and duplications;
e) existence of procedure for keeping data on storage support for minimum 10 years;
f) ensure the possibility to reintegrate in the system the archived data;
g) the restoration procedure used;
h) the existence of periodic refresh procedure of archived data;
i) the existence of the prohibition to update, insert or delete data in specified circumstances (for example, for a financial management and accounting application, the prohibition may be for deleting accounts from a closed period);
j) the existence and completeness of the information product documentation;
k) the contract with the software vendor in terms of information product maintenance and update clauses;
l) the version management organization, changes and corrections of computer systems and software;
m) reconciliations performed after data migration, as part of information system replacement or change in the data processing flow;
n) other controls arising from the specific application.

A special category of IT controls relate to compliance of the information system with the requirements imposed by the legislative and regulatory framework. Legislative and regulatory requirements vary from country to country.

These include:

- Private data protection legislation and legislation on personal data protection;
- Law on misuse of computers within the meaning of cybercrime;
- Financial and banking regulations;
- Intellectual property laws.

Regarding controls over information input, output or stored in the database, the following are usual for checking the compliance with regulations of a financial management and accounting application:

- compliance of accounts with the chart of accounts;
- Romanian-language tags of the information contained in the input documents and output statements;
- ban the opening of two accounts with the same number;
- ban the account number change when data were recorded in that account;
- ban the removal of an account for the current or previous year if it contains records or balance;
- respect the legal format for documents and accounting statements generated by the application;

- synthetic balance accuracy resulting from analytical balance; generation for any calendar month;
- reflect the correct transactions in the database, in documents and and output statements;
- existence and accuracy of statements required by law;
- other controls arising from the specific application.

Risk analysis in a computerized environment. Risks generated by operating a computer system, arise from analysis of factors that impact the activity of the audited entity, namely: dependence on the computer system, resources and knowledge in information technology, trust in the computer system, computer system changes, information technology outsourcing, information security, compliance with legal requirements. ***Erorrs and people's negligence*** are the most important sources of problems. To reduce the risks caused by them, the entity must implement controls and procedures to help reduce / eliminate the effects caused by ignoring the issues that determine how the employees use the system, their quality, their motivation at work, the staff turnover, management structure and volume work.

In most cases, the entity does not have an ***integrated computer system***, this being composed of sepparate application implementations, dedicated to specific problems (financial and accounting software application, dedicated core business application, etc.). This type of architecture has disadvantages at user level, as well as a number of impediments such as those related to the difficulty or impossibility of applications interoperability or multiplication of information. Transactions are processed in distinct applications, information entered into the system are validated in a heterogeneous manner: automatic procedure combined with manual procedures to ensure detection and correction of input errors, and detection of data inconsistencies or redundancy. Lack of an integrated solution is also reflected in the existence of different databases, some residing on obsolete hardware/ software platforms, different and sometimes inadequate user interfaces, reduced communication facilities and security issues with associated risks.

The high degree of fragmentation of the computer system involves frequent user actions during the processing flow and influences in respecting the document flow, which greatly increases the risk of error. Depending on the implemented architectural solution and on the initial estimates regarding the size of the database and processing complexity, a system can "resist" or not to significant increases in the volume of transactions generated by changes in the entity. Estimating the risk that in the near future, the computer system can not support ***increasing volumes of transactions*** involves taking important decisions at management level, within the meaning of its redesign, and thus the allocation of an appropriate budget.

System configuration changes must be authorized, tested, documented and controlled.

1. Typical abnormalities in operating the computer system

The most common abnormalities in the operation are:

(a) applications are not running correctly due to incorrect operation of the software or use of an incorrect version, incorrect configuration parameters entered by the operating personnel (e.g., system clock and date set incorrectly can cause errors in calculating interest, penalties, wages, etc..).

(b) ***loss or alteration of financial applications or data files*** can result from misuse or unauthorized use of utilitary programs

(c) ***IT personnel does not know how to handle problems or reporting errors*** and the attempt to solve them by themselves can cause even greater losses;

(d) ***Delays and processing interruptions*** due to setting inappropriate priorities tasks scheduling;

(e) ***Lack of backup and planning of probable incidents*** increase the risk of inability to continue working after a disaster.

(f) ***Lack of system capacity (resources)***, the system being unable to process transactions due to overloading.

(g) ***The growing time of system unavailability until remedy the error.***

(h) ***unresolved user issues*** due to malfunctioning of Helpdesk application.

In a computerized environment, the magnitude of risks takes another dimension, their nature is influenced by a number of factors specific to information technology use:

a) ***The information density*** is much higher than conventional systems based on paper.

b) ***Lack of entry documents*** - data can be entered into the system without being based on evidence - is an example of on-line transactions systems.

c) ***Lack of visible "traces" of transactions*** - Though in the practice of manual processing, any transaction can be traced starting from the primary document, then the books and accounts - in automatic processing, the route of a transaction may exist for a limited period of time, in electronic format.

d) ***Lack of visible output*** - certain transactions or results, especially when these represent details, can be retrieved memorized only in the application files (not in printed form).

e) ***Transparency of documents*** related to the conduct of operations. Diskettes, optical disks and other modern media that are used to save large volume of information, amounting to tens of thousands of pages, can be discreetly subtilized generating fraud or at least affecting the confidentiality of such information.

f) ***Authorization of transactions***. In a computerized environment, the computer's ability to automatically initiate and execute some transactions can be included ; in other words, it is the design of applications that may have incorporated certain defalut authorization and automatic generation functions.

g) ***Uniform transaction processing***. A computer application processes uniformly similar transactions Thus, document inputting errors associated with manual processing are virtually eliminated. However, programming errors may lead to incorrect processing of transactions, so that auditors will focus on accuracy and consistency of output.

h) ***Unauthorized access to data and files*** can be performed with greater ease, which implies a great potential for fraud and error.

i) ***Retention of data storage media***, can be a safe way that unauthorized stakeholder take possession of valuable information

j) ***Data aggregation***. New automatic data processing systems, such as those assisting the decision making process, led to capitalizing of important information of the entity, generating forecasts and strategy in a given field. Thus, information gains more facets.

The evolution of information technology has witnessed an accelerated pace during the past years, but not the same can be said about the progress in data security. The deep integration of systems is a consequence of improving the means of communication and proliferating computer networks. E-commerce applications are just one example, but it can be said that they have opened even more the appetite of the "specialists" in the ***informational fraud***.

Lack of trace of possible criminal attacks is another worrying element of the new working environment ; in effect, data updates, addition or deletion operations have become much easier to operate, but at the same time, difficult to detect. The objective of information risk analysis (IT risks) is to identify means trough which data and, consequently, the information system that contains them, is exposed to risk.

5. CONCLUSIONS

Items listed lead to the idea that computerized environment poses new risks and any organization, to ensure effective protection of information, has to develop a complex process of risk analysis and study. The risk posed by information technology usage is manifested through its own components: threat, vulnerability and impact. Threats exploit vulnerabilities of a system and actually causing the impact, the combination of these three elements determine the size of risk. The risk level of an organization can not be eliminated, it will always exist, the company’s management being responsible for reducing it to an acceptable level.

REFERENCES:

[1]. Arens, A.; Loebbecke, J. (2003) *Audit - o abordare integrată,* Editura ARC

[2]. Călin, O.; Ristea, M. (2004) *Bazele contabilităţii,* Editura Didactică şi Pedagogică

[3]. Popa, Ş.; Ionescu, C. (2004) *Towards Online Auditing.The database Environment*, 2-nd International Seminar on IT Audit, Nanjing

[4]. Popa, Ş.; Ionescu, C. (2005a) *Audit în medii informatizate,* Editura Expert, Bucureşti

[5]. Popa, Ş.; Ionescu, C. (2005b) *Auditul sistemelor informatice*, Tribuna Economică, Revista Controlul Economic şi Financiar, Nr.9, Bucureşti

[6]. Popa, Ş.; Ionescu, C. (2005c) *Tehnologia informaţiei în auditul extern*, Tribuna Economică, Revista Controlul Economic şi Financiar, Nr.3, Bucureşti

[7]. Ristea, M.; Dumitru, C. (2005) *Contabilitate aprofundată,* Editura Universitară

[8]. Camera Auditorilor din România (2005) *Audit financiar 2005 - Standarde. Codul privind conduita etică şi profesională*

[9]. *IASB - Standarde Internaţionale de Raportare Financiară,* Editor CECCAR, Bucureşti

[10]. *Contabilitatea, Expertiza şi Auditul Afacerilor,* Editor CECCAR, Bucureşti

[11]. Declarația internațională privind practica de audit 1001 - *Medii IT - calculatoare neincluse în rețea*

[12]. Declarația internațională privind practica de audit *1002 - Medii IT - sisteme computerizate on-line*

[13]. Declarația internațională privind practica de audit *1003 - Medii IT - sisteme de baze de date*

[14]. Declarația internațională privind practica de audit 1008 **-** *Evaluarea riscurilor şi controlul intern - caracteristici şi considerente privind CIS*

[15]. Declarația internațională privind practica de audit 1009 - *Tehnici de audit asistate de calculator*

[16]. *IS Standards, Guidelines and Procedures for Auditing and Control Professionals*, ediția februarie 2010, *www.isaca.org*