Extended Residual Aggregated Risk Assessment – A Tool For Managing Effectiveness of the IT Audit

TRAIAN SURCEL,
CRISTIAN AMANCEI,
ANA-RAMONA BOLOGA
ALEXANDRA FLOREA
RAZVAN BOLOGA
Computer Science Department
Academy of Economic Studies from Bucharest
Pta. Romana no. 6, Bucharest
Romania
tsurcel@ie.ase.ro, cristian.amancei@ie.ase.ro, bologa.ramona@ie.ase.ro,
alexandra.florea@ie.ase.ro, razvanbologa@ase.ro
http://www.ase.ro

Abstract: -This paper proposes an audit methodology which aims to identify key risks that arise during the IT audit within an organization and presents the impact of identified risks. This involves evaluating the organization's tolerance to IT systems unavailability, identifying auditable activities and subtasks, identifying key risk factors and the association of weights, evaluating and classifying significant risks identified, conducting audit procedures based on questionnaires and tests and assessing the remaining aggregate risk that was not reduced by effective controls. Verifying the existence of compensating controls and the possibility of their implementation in an iterative manner, followed by a reassessment of covered risks, after each iteration, eventually provides an insignificant remaining aggregate risk. The development of the audit mission has to be correlated with the corporate governance requirements, the quality assurance and marketing the audit function. The results obtained are evaluated by taking into consideration the confidentiality and integrity of resources involved.

Key-Words: - IT audit, audit methodology, risk factors

1 Introduction

Research on risk has moved from an approach based on the negative dimension of risk to a complex approach in which risk is seen both as a threat and as an opportunity. The present research follows this new direction, aiming to make more efficient the management of risks identified during the audit process.

The audit methodology presented in this paper aims to identify key risks that arise during the IT audit within an organization, regardless of the organization's activity, and to present the impact of the identified risks.
The purpose of this methodology is to reduce the time assigned to risk identification during an audit mission, seeking more efficient use of resources. The use of a predefined risks matrix is an important factor, contributing to increased efficiency of resource use in the audit engagement.

2 Methodology

After analyzing practices in the field of IT controls ([1], [2], [3], [4]) developed by renowned organizations in this area, we propose to implement the IT audit process based on a methodology that follows the next steps:
1. organizational tolerance to IT systems unavailability;
2. identifying activities and sub activities that can be audited;
3. risk factors and associated weights;
4. level, total score and ranking of significant risks;
5. conducting audit procedures based on questionnaires and tests;
6. residual aggregate risk assessment.

2.1 Organizational tolerance to IT systems unavailability

One of the most important efficiency indicators of an information system is response time, which represents the time interval between the moment when a request is launched and the moment when the answer to the request is received.

Response time is determined based both on basic functional components such as queries, but also on complex components up to the levels of subsystems and information system. Maximum permissible limit by

which the organization can operate without the support of the information system is represented by the level of unavailability.

The first step towards IT audit within an organization is to establish the level of service unavailability that the IT department must provide within the organization, level that depends on: activity profile of the organization, the support the IT department provides in carrying out main activities of the organization (e.g.: production, sales or office work), the importance of assets held by the IT department.
Based on these criteria, we have the categories presented in Table 1.

Table 1: Organizations according to tolerance shown to IT systems unavailability

Category	Tolerance to IT systems unavailability
Organizations with very critical IT systems	<2 working days
Organizations with critical IT systems	2-4 working days
Organizations with non-critical IT systems	>4 working days

2.2 Identifying activities and sub activities that can be audited

The organization's tolerance level to the unavailability of IT systems has direct implications on the resources assigned to IT. As the organization's tolerance to the unavailability of IT systems increases, the level of resources allocated to this department decreases.

As a result, the composition of auditable areas must be correlated with the resources allocated to the IT department. For this reason we have developed a structure of auditable IT domains and sub domains for each category, structure that is presented in the following table.

Next we present the IT activities and sub activities that can be audited, according to the category of the organization.

I. IT strategic plan with the following subtasks:
- I.1 Organizational policies in the IT field
- I.2 Short-term IT strategy
- I.3 Long-term IT strategy
- I.4 IT budget
- I.5 Information systems used for the main functions of the organization
- I.6 Integration of implemented information systems
- I.7 Performance indicators for the IT department

II. Organization and functioning of the IT department with the following subtasks:
- II.1 Organization chart of IT department
- II.2 Job descriptions for each position within the IT department
- II.3 Qualification and training of employees, including continuous training in the field
- II.4 Employee performance evaluation system
- II.5 Separation of activities at IT department level

III. IT systems with the following subtasks:
- III.1 Procedures for managing access to IT systems, change management in applications and incidents handling
- III.2 Detailed Network Diagram
- III.3 Network Diagram
- III.4 Hardware and network architecture
- III.5 Use and operating manuals
- III.6 Licensing situation
- III.7 Training users of IT systems
- III.8 Monitoring the use of the systems by the administrator
- III.9 Control of correct data processing in applications
- III.10 Contracts with suppliers
- III.11 Monitoring and assessing primary services

IV. IT security with the following subtasks:
- IV.1 IT security procedures
- IV.2 Monitoring the implementation of IT security policy and procedures
- IV.3 Physical controls in IT
- IV.4 Information classification
- IV.5 Security of network access and the data exchanged through the network
- IV.6 Antivirus and firewall
- IV.7 Backup management
- IV.8 Business continuity plan
- IV.9 Disaster recovery plan

2.3 Risk factors and associated weights

General methodological rules ([5] [6] [7]) recommend for risk analysis the use of three risk factors or criteria, which cover all auditable activities, namely:
- Assessment of internal control;
- Quantitative assessment;
- Qualitative assessment.

For establishing the weight of risk factors, the importance and weight of the risk factor in the organization's activities is considered. Note that the sum of the weights of the risk factors should be 100.
The weights of the risk factors are established by the audit team based on their experience, taking into account the specific of the audited organization, according to the model shown below.

The considered risk factors are general factors that cover any entity; they can be customized if the situation encountered at the customer demands it.

Table 2: Determining risk factors, weights and levels of risk assessment

Risk factors (F_i)	Risk factors weight (P_i)	Risk assessment level (N_i)		
		N_1	N_2	N_3
Assessment of internal control F1	P1 – 40%	There are procedures and they are applied	There are procedures but they are not applied	There are no procedures
Quantitative assessment F2	P2 – 35%	Low financial impact	Medium financial impact	High financial impact
Qualitative assessment F3	P3 – 25%	Low Vulnerability	Medium Vulnerability	High Vulnerability

2.4 Level, total score and ranking of significant risks

To establish the risk level, a three levels scale of values has been used for the three risk factors mentioned above: the assessment of internal control (F1), quantitative assessment (F2), qualitative assessment (F3).

During this stage, significant risks associated to each auditable subtask will be identified by the auditors, according to [8]. For each risk, the impact on the organization in terms of the previously identified risk factors will be evaluated.

In elaborating this analysis the best practices in the field were considered, and they were applied to an organization that has a tolerance to unavailability of IT systems of maximum 2 days.

For risk classification, an equal division of the time interval that may fall within the total score (1-3) was considered, as follows:
- low risks if their total score is in the 1,0 - 1,7 range;
- medium risks if their total score is in the 1,8 - 2,2 range;
- high risks if their total score is in the 2,3 - 3,0 range.

Given the four categories of auditable activities and the auditable sub activities within each category, following is their analysis based on risk factors and establishing a total score. To exemplify this, we considered activity 1, IT Strategic Plan and its sub activities.

Table 3: Significant risks and their score for auditable subtasks of activity 1

Sub tasks	**Significant risks**	**Criteria for risk analysis**			**Total score**
		F1	**F2**	**F3**	**ΣF_i*P_i**
I.1	Not drawing up policies for IT	3	2	3	2.65
	Not delegating responsibilities through the policies	2	2	3	2.25
	Employee ignorance of the policies that apply	2	2	3	2.25
	Failure to update policies	2	2	2	2
I.2	Lack of long-term strategy	2	2	2	2
	Lack of short-term strategy	1	3	2	1.95
	No correlation of short-term strategy with long-term strategy	2	2	2	2
I.3	No correlation between the objectives of the strategy	1	3	2	1.95
	No allocation of the necessary resources	1	3	3	2.2
I.4	No correlations between the budget ant the long and short term strategies	1	3	2	1.95
	Allocation of insufficient resources for the approved projects	1	3	2	1.95
I.5	Unfulfillment of main business functions through appropriate information systems	2	3	2	2.35
	Not following the deadlines for the realization/ modification of the systems	2	2	3	2.25
	No allocation of the necessary resources	1	3	3	2.2
I.6	Lack of procedures for monitoring the transfer / interfaces between systems	3	3	3	3
	Lack of monitoring of transfers / interfaces between systems	2	2	3	2.25
	No analysis of the incidents that occurred during monitoring in order to identify and eliminate the causes which have led to their appearance	2	2	3	2.25
I.7	Lack of performance tracking indicators	3	2	3	2.65
	Lack of monitoring of performance indicators	1	2	2	1.6
	No measures are taken for indicators to fit the parameters	2	2	2	2
II.1	The department's organizational chart is not approved	3	2	3	2.65

	The department's organizational chart is not updated/completed	2	2	2	2
II.2	Job descriptions are not filled/signed by the employees	3	3	3	3

These risks will be used in the development of the audit questionnaire that will be used during the audit mission for the client systems and processes evaluation.

2.5 Conducting audit procedures based on questionnaires and tests

Control testing is made by audit procedures that will follow two main aspects [9]:
a) Evaluating the design effectiveness of internal controls;
b) Evaluating the operability of internal control.

Audit procedures that target the design effectiveness of internal controls evaluate if these controls are properly designed to prevent vulnerabilities in the IT systems. Audit procedures oriented towards control operability focus on determining how controls were applied, the consistency with which they were applied and who applied them. In addition to questions to the qualified staff and observation of the application of controls, when these controls are tested, the IT auditor has to recreate the functioning of controls.

In conducting the audit, audit questionnaires will be developed to address all identified risks for the auditable tasks and subtasks. Assessment of risk cover through controls will be made based on the responses to questionnaires and on the results of audit procedures testing.
Testing will apply in all cases where samples can be constituted. The sample will be 15% of the population but not more than 20 entries.

For some of the significant risks identified in table 3, we developed a questionnaire to complete the model.
For each question in the survey the respondent will have two options: affirmative/negative.

Table 4: Sample questions from the survey for the partial study of the identified significant risks

Significant risk	Questions
Not drawing up policies for IT	Are there IT policies drawn?
Not drawing up policies for IT	Have the IT policies been approved by the organization's management?
Not delegating responsibilities through the policies	In these policies are there clearly defined the objectives and measures that must to be implemented?
Not delegating responsibilities through the policies	Are there management structures to administer and monitor the reach of these objectives?
Employee ignorance of the policies that apply	Is there a process through which the employees are familiarized with the IT policies and the changes these introduce?
Failure to update policies	Are policies regularly updated?
Lack of long-term strategy	Is there a long term strategic plan developed?
Lack of short-term strategy	Are there strategies developed for each department and to they support the strategic plan?
Lack of long-term strategy	Is the strategic plan covering all the processes taking place within the organization?
Lack of short-term strategy	Was the strategic plan approved by the leadership of the organization?
No correlation of short-term strategy with long-term strategy	Do activities undertaken by short-term strategy serve the long-term strategic plan?
No correlation between the objectives of the strategy	Were the deadlines for achieving the proposed objectives correlated through strategy?
Lack of short-term strategy	Is there a short term strategic plan developed?
Lack of short-term strategy	Is there a process to verify the completion stage of the strategy?
No allocation of the necessary resources	Are the necessary resources for each element of the strategy identified and allocated?
No correlations between the budget ant the long and short term strategies	Are the budgeted financial resources needed for achieving the short and long term strategies well documented?
Allocation of insufficient resources for the approved projects	Are the necessary resources for each approved project identified and planned?
Unfulfilment of main business functions through appropriate information systems	Are the main functions of the organization covered by information systems according to needs?
Unfulfilment of main business functions through appropriate information systems	These systems use a technology for which there is support available on the market?
Not following the deadlines for the design/modification of the systems	Were the deadlines for designing/modifying of support systems for the organization's functions established and monitored through the short term strategy?
No allocation of the necessary resources	Are there resources assigned to maintain and develop information systems used by organization's core functions?
Lack of procedures for monitoring the transfer / interfaces between systems	Are procedures developed and approved to monitor transfers / interfaces between systems?
Lack of procedures for monitoring the transfer / interfaces between systems	Developed procedures cover all transfers / interfaces between systems?

Lack of monitoring of transfers / interfaces between systems	Transfers / interfaces between systems are regularly monitored?
Lack of monitoring of transfers / interfaces between systems	Incidents / errors occurred during the monitoring of transfers / interfaces between systems are classified and reported?
No analysis of the incidents that occurred during monitoring in order to identify and eliminate the causes which have led to their appearance	The incidents occurred during the monitoring of transfers/ interfaces between systems are analyzed and action plans are developed and implemented to remove the causes?
Lack of performance tracking indicators	The organization has defined and agreed indicator for performance tracking of IT department?
Lack of monitoring of performance indicators	IT department's performance indicators are monitored regularly?
No measures are taken for indicators to fit the parameters	An action plan for indicators to meet the established thresholds is developed and implemented?
The department's organizational chart is not approved	Is there an official organizational chart approved by the leadership of the organization?
The department's organizational chart is not approved	Are all management positions occupied?
The department's organizational chart is not updated/completed	Is the department's organizational chart updated periodically?
The department's organizational chart is not updated/completed	Are all operational positions occupied?
The department's organizational chart is not updated/completed	Are measures taken to fill in vacancies?
Job descriptions are not filled/signed by the employees	Are there job descriptions for all the staff that clearly define the scope of obligations?
Job descriptions are not filled/signed by the employees	Are the job descriptions signed by the job holders?
Job descriptions are not filled/signed by the employees	Do job descriptions include daily duties and responsibilities of employees?

2.6 Residual aggregate risk assessment

After testing the controls through the above mentioned methods we can calculate the remaining aggregated risk as the risk that was not reduced by effective controls. For risks not covered by effective checks the following steps are performed:

a) the existence of compensatory controls or the possibility of implementing a new automated control is verified;

b) a new evaluation of the risks covered by ineffective controls is performed.

This process is repeated, usually until we reach the conclusion that no more compensatory controls can be found or that the aggregate risk remaining is insignificant.

First we calculate the residual aggregate risk for each auditable activity using the following formula:

$$RA_k = \frac{\sum R_i}{\sum R_j} \quad (1)$$

where:

R_i - total score for risks not covered by effective controls;

R_j - total score for each risk;

i - total number of risks not covered by effective controls;

j - total number of significant risks;

k - total number of auditable activities;

RA_k - residual aggregate risk for activity k.

All areas included in the audit scope have to be evaluated, by using the audit questionnaire. Due to this reason, in the end we calculate the total residual aggregate risk with the following formula:

$$R = \frac{\sum RA_k}{k} \quad (2)$$

where:

RA_k - aggregate risk for activity k;

k - total number of auditable activities;

R - total residual aggregate risk.

After calculation of indicators the results of the audit are assessed. The criteria that must be met in order to issue an unqualified opinion are:

a) all high risk (scores above 2.3) should be covered by effective checks;

b) residual aggregate risk for each auditable activity should not pass the threshold of 0,3;

c) total residual aggregate risk should not pass the threshold of 0,2.

If any of the above mentioned criteria is not met the opinion issued will be qualified.

3 Implementation of audit methodology

To implement the proposed methodology we chose to develop a web application developed in PHP using a MySQL database.

The application was developed on three distinct levels:

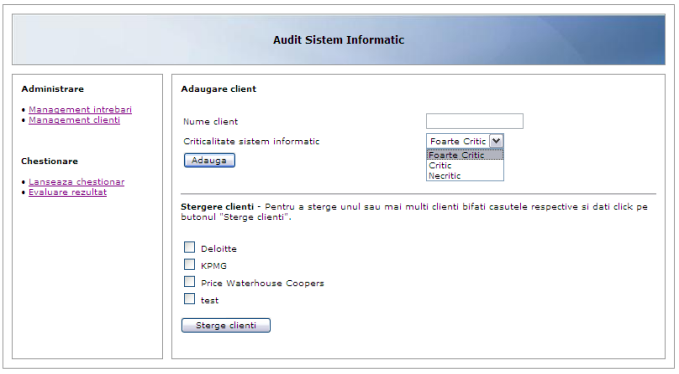
- Level 1, a database with question and answers from the users;
- Level 2, a web server providing HTML pages. It is installed on the same machine as Level 1 but it runs independently;

- Level 3, the client, any browser - the application is designed to run in both Internet Explorer(various versions) and in Mozilla Firefox.

The application was developed to follow the steps described in the methodology, as follows:

A. The first step the user must take is to create a client that will be classified on the basis of tolerance to non-availability of IT systems, according to table 1.

Figure1. Creating the client that will be classified



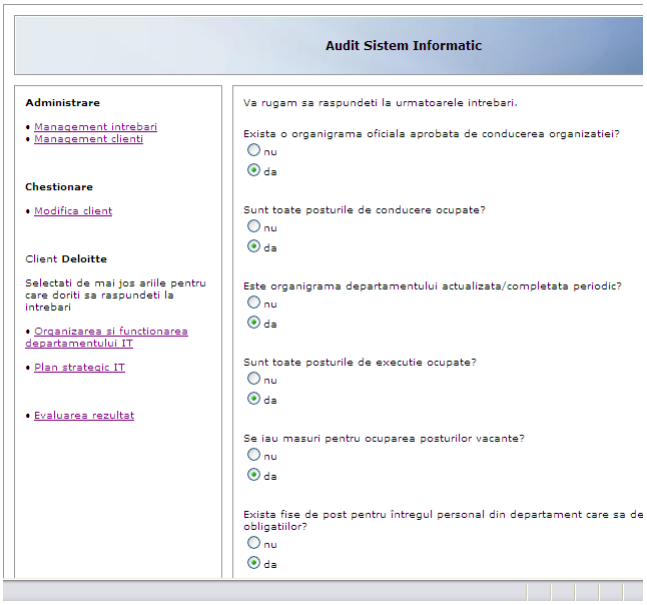
B. If the audited organization is already in the system, we proceed to its selection in order to complete the questionnaire.

C. Completing the questionnaire is carried out for each audited area as follows:

- Organization and functioning of the IT department;
- IT strategic plan.

For each audited activity the questions from the survey defined in table 4 have been loaded.

Figure 2. On-line questionnaire



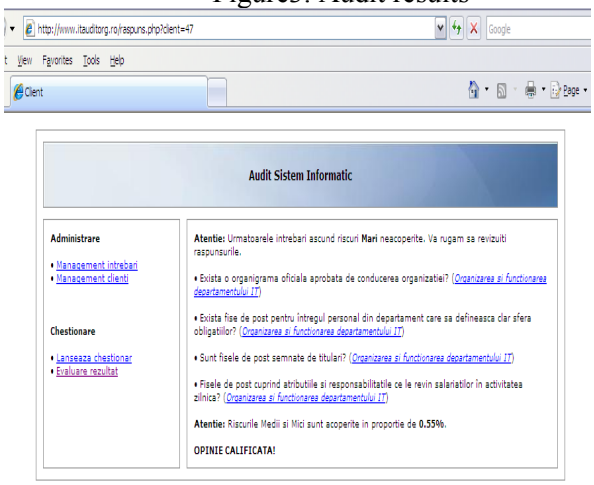
D. For easier administration of the application a separate module for loading questions was created. This module is necessary in order to facilitate changes of questionnaire by users without administrator intervention

E. Assessment of the audit results is made according to the requirements in paragraph 2.6, by comparing the results obtained from indicators evaluation with the predefined levels:

- all high risk (scores above 2.3) should be covered by effective checks;
- residual aggregate risk for each auditable activity should not pass the threshold of 0,3;
- total residual aggregate risk should not pass the threshold of 0,2.

The result of the assessment can be an unqualified opinion (without problems). If one of the criteria is not met the result is a qualified opinion.

Figure3. Audit results



When the results of the audit are a qualified opinion, the client is warned of the activities were problems were identified (risks not covered properly) in order to review these activities.

The client has to be properly informed of the issues identified during fieldwork, and necessary time is given to remediate the problems that can be resolved on short term, and a reassessment is preformed before the final conclusion is given.

4 Increasing the management of IT Audit effectiveness

The Residual Aggregated Risk Assessment (RARA) procedure needs to be integrated as part of the methodology of the IT System Audit to offer to the

management team some tools for increasing the effectiveness of the IT audit activities. The effectiveness of the IT audit means in the real practices, first of all, to fix with accuracy, precisely, as much as possible, the audit objectives, the area of auditable activities and controls, and the background information usefully for the audit workpapers.

Thru the selection of the auditable activities based on the RARA algorithm, it can be reduced the duration of the entire audit mission, the resources spent with the audit, this means reducing costs, do not overload the budget, and of course a honestly task assignment on the audit team members and also on the personal and company stuff.

The success on using the Residual Aggregated Risk Assessment Procedure, together with other IT audit management tools depends closely of the ability of the audit team to correlate the developing the audit mission with the corporate governance requirements, with audit quality assurance and marketing the audit function.

The corporate governance requirements in connection to the applied RARA procedure are linked with the stipulation of the model of principles proposed by the Corporate Governance Center at Kennesaw State University, Georgia [10], and endorsed by IIA. From this model, we select the following principles: interaction, board purpose, board responsibilities, expertise, meeting and information.

Interaction principle requires effective interaction among the board, management and the auditor. Board purpose principles suggest that board of directors should understand that the purpose is to protect the interests of the corporation's stakeholders also by developing and repeating regularly audit procedures. Board responsibilities principle refers to the monitoring of the corporation's strategy including monitoring risks and the control system by the management stuff and chief executive officer. Expertise principle claims that the directors should posses even audit background knowledge to the sure they achieve and maintain the necessary level of expertise for all area of responsibilities [11]. Meeting and information principle underline the obligation to the board to meet frequently and share information with the audit committee about the progress and the results of the audit process.

Respecting these principles in audit practice brings mare efficiency to the audit management. The audit procedures will be much more clearly defined, understand by the employee and the stuff, and much more easy to watch and check and finally accepted and put it in practice. All these happened because all the involved persons become part of the expanded audit teamwork.

The quality assurance provides a similar service to the audit as that audit provides to the management. In terms of quality assurance it must be established a quality control program to ensure that all assignments for auditors are completed and activities are well evaluated and monitored.

The Residual Aggregated Risk Assessment is a dynamic procedure because the organization tolerance to the IT systems unavailability, the risk factors, the importance and the impact of the risk factors on the business performed by the organization and the weights of the risk factors are changing fast under the pressure of changes of hardware, software and business environment. For this reasons keeping quality assurance at a high level means updating of the matrix of risks assessment, reevaluating the weights and residual risks, updating the list of auditable activities and subactivities and even the set of questionnaires. We need to have a good informational support to manage the audit process. As any management process, the IT audit management uses the planning, organizing, coordination, and control attributes. The quality assurance [12] in managing the IT audit generates a series of responsibilities for the director of auditing to maintain active a quality control program based on detailed checklist with documents, information circuits for these documents, assignments for audit member's team, intermediate evaluations and finally reports. Based on this quality control [13] program the manager can do a better planning supervision, verifying if the work is properly planned and workpapers are complete. Using the result of the Residual Aggregated Risk Assessment and other audit procedures a detailed recommendation are produced, containing statement off conditions, criteria, cause, effect and statement of action. In this way we close the feedback of current audit mission and after a while a new audit cycle will begin but under different circumstances, new audit area, budget, timing of audit and auditors assigned.

An interesting aspect needed to be underlined as a success factor for managing the effectiveness of the IT audit and applying the Residual Aggregated Risk Assessment procedure, is to understand the marketing of the audit function. The recommendations formulated by the audit team represents nothing else than services delivered to the costumer, the beneficiary organization. We must think the development of our audit analyzes also from the marketing perspective. From our point of view, for the residual aggregated risk assessment

procedure it's necessary to establish, into an explicit manner, the activities and risks mentioned foreword in table 2 and table 3 and in the same time it's necessary to establish the item of the questioner in table 4 and grouping this items in accordance with the potential customers needs and expectations. The final audit report must be build to mitigate these expectations. To get in more details on this direction of the marketing of audit function, our questioner and interviews must be build, by taking into account the customers profiles.

This profiles offer us information about task assignments, job responsibility and duties, for the employers and managers. In this way the audit mission, generally speaking, will be much better received from the company personal.

All this more or less theoretical aspects, underline the necessity that any audit procedure, in our case the extended residual aggregated risk assessment procedure, must not be mechanical take over, this procedures must be included into a global approach of the IT audit methodology.

5 Methodology extension by taking into account the confidentiality and integrity

Due to the fact that the methodology presented above takes into consideration, as a primary factor, the resources availability, in this chapter we present the extension of the methodology by taking into account the resources confidentiality and integrity, according to [3].
The following steps are proposed to be performed for the low and medium risks that are not covered by effective controls, in order to evaluate the impact of confidentiality and integrity loss [14]:

A. First the resources affected by those risks are evaluated. The resources are classified as: software, hardware, paper documentation, infrastructure, people and records (information files).

B. For each one of these resources affected, we identify the threats and vulnerabilities to which they are exposed.

Table 5: Risk analysis example for confidentiality and integrity

Resource	Threat	Vulnerability	Criteria affected
Software	Software error	1. Lack of testing	C, I
		2. Incompatibility with O.S.	I
		3. Outdated application	C, I
	Processing errors	4. Lack of training	C, I
		5. Ambiguous information	I
Hardware	Hardware malfunction	6. Lack of maintenance	I
		7. System overloading	I
Paper documentation	Unauthorized access	8. Lack of protection systems	C, I
Infrastructure	Disaster	9. Lack of alarming systems	C, I
		10. Improper sizing	I
People	Vandalism	11. Unprotected doors and windows	C, I
		12. Lack of backup	I
		13. Unprotected open areas	C, I
Records	Unauthorized interior access	14. Lack of user access controls	C, I
		15. Rights granted wrong	C
	Unauthorized exterior access	16. Network access protection failure	C, I
		17. Lack of user access controls	C, I

C. Evaluation of threat and vulnerability level for each scenario.
The threat levels are:

1. Improbable & no known precedence;
2. Probable to occur once every three years;
3. Probable to occur once every quarter.

The vulnerability levels are:

1. Control is guaranteed to function effectively at every instance of occurrence of the threat;
2. Control is partially effective and would function most of the time in the event of occurrence of a threat;
3. Control is likely to fail at every instance of occurrence of the threat or There is no control in place to mitigate this threat.

D. Value evaluation of the affected assets by taking into consideration the loss of confidentiality and integrity

The integrity levels are:

1. Information can be recovered without major effort;
2. Information can be recovered with major effort;
3. Information must not be altered, it is critical to the business processes.

The confidentiality levels are:

1. Internal information;
2. Internal information with limited access;
3. Confidential information.

E. Risk assessment is performed, based on the values defined above, by using the following formula:

Risk = Threat x Vulnerability x Resource Value

where:

Resource Value = (C + I) / 2

Threat and vulerability	T	V	C	I	RV	Risk
1	2	3	2	2	2	12
2	3	2	2	2	2	12
3	2	2	2	3	2,5	10
4	2	3	2	3	2,5	15
5	3	3	3	2	2,5	22,5
6	3	2	3	2	2,5	15
8	3	2	3	3	3	18
9	2	3	3	3	3	18
10	2	3	3	2	2,5	15
11	2	3	2	2	2	12
12	2	2	2	3	2,5	10
13	3	2	2	3	2,5	15
14	3	2	2	2	2	12
15	3	3	3	2	2,5	22,5
16	2	3	3	2	2,5	15
17	2	2	2	3	2,5	10

The obtained risk levels are classified as it fallows:

- Low risks: 1 - 9;
- Medium risks: 10 - 18;
- High risks: 19 - 27.

The obtained high risks have to be treated by the audited organization by implementing additional controls.

Due to the high resource allocation that has to be performed by the auditor in order to realize the risk assessment by using confidentially and integrity, the audited organization has to agree to this approach, as it will increase the costs of the audit mission.

6 Conclusion

The approach to the conduct of the audit process and evaluating the results proposed in this paper aims to improve the audit process by reducing its duration and increasing the competitiveness of the obtained result.

The new methodology is based on both research conducted by authors and fundamental elements taken from specialty literature.

Generally, by conducting an IT audit leads to a raise of the trust level of an organization. Other factors that advocate for the use of the new methodology are:

- the large scale of information system usage in order to support processes within an organization;
- choosing a system which gives high confidence to business partners and that allows the organization to operate to the highest standards;
- the necessity of certification of the information security level offered by systems implemented within the organization.

The extension of the approach by taking into account the confidentiality and integrity, involves great levels of resources allocation, the acceptance must be obtained from the client, as the results are unpredictable.

References:

[1] *Office of Government Commerce ITIL Lifecycle Publication Suite*, version 3, 2007;
[2] *IT Governance Institute Control Objectives for Information and Related Technology*, v4.1, 2007;
[3] ISO/IEC 27001:2005 *Information technology -- Security techniques -- Information security management systems – Requirements*;
[4] ISO/IEC 27002:2005 *Information technology -- Security techniques -- Code of practice for information security management*;
[5] M. Ghiță, *Auditul intern*, 2nd Edition, Editura Economică, Bucharest, 2009, ISBN: 978-973-709-437-7;
[6] W. Meding, M. Staron, C. Nilsson, *A framework for developing measurement systems and its industrial evaluation*, Information and Software Technology, Vol. 51, Issue 4, 2009, pp. 721-737;
[7] The Institute of Internal Auditors Guidance on Monitoring Internal Control Systems, *Application Techniques*, vol. III, 2008;
[8] S. Schlarman, *IT Risk Exploration: The IT Risk Management Taxonomy and Evolution*, Information Systems Control Journal, Vol. 3, 2009, pp. 27-31;
[9] I. Ivan, G. Noşca, S. Capisizu, *Auditul sistemelor informatice*, Editura ASE, Bucharest, 2005, ISBN: 978-973-594-638-6;
[10] Corporate Governance Center at Kennesaw State University, *21st Governance and Financial Reporting Principles for US Companies,*2002;
[11] Thameral-Rousan, Shahida Sulaiman, Rosalina Abdul Salam, *Supporting Architectural Design Decisions through Risk Identification Architecture Pattern (RIAP) Mode,* WSEAS Transactions on Information Science & Applications, Vol 6 2009, pp 611-620, ISSN:1790-0832;

[12] M. Spremic, *IT Governance Mechanisms in Managing IT Business Value*, WSEAS Transactions on Information Science & Applications, Vol 6, 2009, pp 906-915, ISSN: 1790-0832;
[13] M. Spremic, M. Popovic, *Towards a Corporate IT Risk Management Model*, 6th WSEAS Int. Conf. on Information Security and Privacy, Tenerife, Spain, 2007, pp. 111-116;
[14] N. Azizi, K. Hashim, *Enterprise Level IT Risk Management*, Proceedings of the 8th WSEAS Int. Conf. on Applied Computer Science, 2008, pp. 401-404.