Increasing IT audit efficiency by using a new audit methodology

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.

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Tolerance to IT systems unavailability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizations with very critical IT systems</td>
<td>&lt;2 working days</td>
</tr>
<tr>
<td>Organizations with critical IT systems</td>
<td>2-4 working days</td>
</tr>
<tr>
<td>Organizations with non-critical IT systems</td>
<td>&gt;4 working days</td>
</tr>
</tbody>
</table>

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

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

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 2.4, 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

<table>
<thead>
<tr>
<th>Significant risk</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not drawing up policies for IT</td>
<td>Are there IT policies drawn?</td>
</tr>
<tr>
<td>Not drawing up policies for IT</td>
<td>Have the IT policies been approved by the organization’s management?</td>
</tr>
<tr>
<td>Not delegating responsibilities through the policies</td>
<td>In these policies are there clearly defined the objectives and measures that must to be implemented?</td>
</tr>
<tr>
<td>Not delegating responsibilities through the policies</td>
<td>Are there management structures to administer and monitor the reach of these objectives?</td>
</tr>
<tr>
<td>Employee ignorance of the policies that apply</td>
<td>Is there a process through which the employees are familiarized with the IT policies and the changes these introduce?</td>
</tr>
<tr>
<td>Failure to update policies</td>
<td>Are the policies regularly updated?</td>
</tr>
<tr>
<td>Lack of long-term strategy</td>
<td>Is there a long term strategic plan developed?</td>
</tr>
<tr>
<td>Lack of short-term strategy</td>
<td>Are there strategies developed for each department and to they support the strategic plan?</td>
</tr>
<tr>
<td>Lack of long-term strategy</td>
<td>Is the strategic plan covering all the processes taking place within the organization?</td>
</tr>
<tr>
<td>Lack of short-term strategy</td>
<td>Was the strategic plan approved by the leadership of the organization?</td>
</tr>
<tr>
<td>No correlation of short-term strategy with long-term strategy</td>
<td>Do activities undertaken by short-term strategy serve the long-term strategic plan?</td>
</tr>
<tr>
<td>No correlation between the objectives of the strategy</td>
<td>Were the deadlines for achieving the proposed objectives correlated through strategy?</td>
</tr>
<tr>
<td>Lack of short-term strategy</td>
<td>Is there a short term strategic plan developed?</td>
</tr>
<tr>
<td>Lack of short-term strategy</td>
<td>Is there a process to verify the completion stage of the strategy?</td>
</tr>
<tr>
<td>No allocation of the necessary resources</td>
<td>Are the necessary resources for each element of the strategy identified and allocated?</td>
</tr>
<tr>
<td>No correlations between the budget ant the long and short term strategies</td>
<td>Are the budgeted financial resources needed for achieving the short and long term strategies well documented?</td>
</tr>
<tr>
<td>Allocation of insufficient resources for the approved projects</td>
<td>Are the necessary resources for each approved project identified and planned?</td>
</tr>
<tr>
<td>Unfulfilment of main business functions through appropriate information systems</td>
<td>Are the main functions of the organization covered by information systems according to needs?</td>
</tr>
<tr>
<td>Unfulfilment of main business functions through appropriate information systems</td>
<td>These systems use a technology for which there is support available on the market?</td>
</tr>
<tr>
<td>Not following the deadlines for the design/modification of the systems</td>
<td>Were the deadlines for designing/modify of support systems for the organization’s functions established and monitored through the short term strategy?</td>
</tr>
<tr>
<td>No allocation of the necessary resources</td>
<td>Are there resources assigned to maintain and develop information systems used by the organization's core functions?</td>
</tr>
<tr>
<td>The department’s organizational chart is not approved</td>
<td>Is there an official organizational chart approved by the leadership of the organization?</td>
</tr>
<tr>
<td>The department’s organizational chart is not approved</td>
<td>Are all management positions occupied?</td>
</tr>
<tr>
<td>The department’s organizational chart is not updated/completed</td>
<td>Is the department’s organizational chart updated periodically?</td>
</tr>
<tr>
<td>The department’s organizational chart is not updated/completed</td>
<td>Are all operational positions occupied?</td>
</tr>
<tr>
<td>The department’s organizational chart is not updated/completed</td>
<td>Are measures taken to fill in vacancies?</td>
</tr>
<tr>
<td>Job descriptions are not filled/signed by the employees</td>
<td>Are there job descriptions for all the staff that clearly define the scope of obligations?</td>
</tr>
<tr>
<td>Job descriptions are not filled/signed by the employees</td>
<td>Are the job descriptions signed by the job holders?</td>
</tr>
<tr>
<td>Job descriptions are not filled/signed by the employees</td>
<td>Do job descriptions include daily duties and responsibilities of employees?</td>
</tr>
</tbody>
</table>

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:

\[ R_{Ak} = \sum \frac{R_i}{\sum R_j} \]  

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;
- \( R_{Ak} \) - residual aggregate risk for activity \( k \).

In the end we calculate the total residual aggregate risk following the formula:

\[ R = \sum \frac{R_{Ak}}{k} \]

where:
- \( R_{Ak} \) - 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.

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.

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.

a) The result of the assessment can be an unqualified opinion (without problems)  
b) If one of the criteria is not met the result is a qualified opinion.
When the results of the audit are a qualified opinion, the user is warned of the activities were problems were identified (risks not covered properly) in order to review these activities.

4 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 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.

References: