Abstract: the purpose of this paper is to present a method of using the risks assessment during IT audit of an organization, regardless of the organization activity, and presenting the impact of using questionnaires during the audit mission. The changes in the current economical environment, involves rapid changes from the economic partners in order to provide services at the efficiency requested by the market. The use of predefined questionnaires and risk matrix can help the services providers to adapt to the market and maintain the service quality.

Key-Words: IT risk, risk assessment, aggregated risk, audit methodology, audit questionnaires

1 Introduction

In [1], we presented the implications of using organizations tolerance to the IT systems availability in audit risk assessment. This approach presented in [1] considers the level of service availability that the IT department needs to ensure within the organization. The maximum permissible limit until the organization can operate without the support of the information systems will be classified in the following levels:

<table>
<thead>
<tr>
<th>Category</th>
<th>Tolerance to the IT systems availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizations with critical IT systems</td>
<td>&lt;2 working days</td>
</tr>
<tr>
<td>Organizations with medium IT systems</td>
<td>2-4 working days</td>
</tr>
<tr>
<td>Organizations with uncritical IT systems</td>
<td>&gt;4 working days</td>
</tr>
</tbody>
</table>

Given the existence of a correlation at the organization level, between the availability of systems and the budget for IT, it is necessary that the composition of the audit areas to be linked to IT department resources. Due to this reason, a structure of areas and subareas to be audited for each organization category has been developed, as presented in the example below:

<table>
<thead>
<tr>
<th>Area</th>
<th>Subarea to be audited</th>
<th>Category</th>
<th>Tolerance to the IT systems availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. IT strategic plan</td>
<td>1.1 Organization policies in IT area</td>
<td>Critical, Medium, Uncritical</td>
<td>X, X</td>
</tr>
<tr>
<td></td>
<td>1.2 Short term IT strategy</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>1.3 Long term IT strategy</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

The risk factors recommended to be used during risk assessment by [2], are:
- internal control assessment;
- quantitative assessment;
- qualitative assessment.

For establishing the weights of the risk factors, the importance and the impact of the risk factors on the business performed by the organization are taken into account, as presented in the table below:

<table>
<thead>
<tr>
<th>Risk factors (F_i)</th>
<th>Risk factors weights (W_i)</th>
<th>Level of risk assessment (L_i)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal control assessment F1</td>
<td>W_1 = 40%</td>
<td>There are procedures and are applied</td>
</tr>
<tr>
<td>Quantitative assessment F2</td>
<td>W_2 = 35%</td>
<td>Low financial impact</td>
</tr>
<tr>
<td>Qualitative assessment F3</td>
<td>W_3 = 25%</td>
<td>Low vulnerability</td>
</tr>
</tbody>
</table>
The risk factors considered are generic risk factors that cover any entity, but they can be customized if the situation encountered in customer demands. The weights of the risk factors are established by the team of auditors, based on the experience, and taking into account the characteristics of the organization audited.

The auditors will identify the significant risks associated with each subarea to be audited. For each risk will assess the impact on the organization in terms of risk factors previously identified.

For risk classification we have considered an equal division of the total score interval (1-3), as it follows:

- low risks if the total score is in the interval 1.0 - 1.7;
- medium risks if the total score is in the interval 1.8 - 2.2;
- high risks if the total score is in the interval 2.3 - 3.0.

Given the activities to be audited and the auditable subareas within each class, we analyzed them by using the criteria (risk factors) and establish a total score for the risks identified by using experience and the best practices [5], [6], an example being presented in the table below:

<table>
<thead>
<tr>
<th>Subarea to be audited</th>
<th>Significant risks</th>
<th>Criteria for risk analysis</th>
<th>Total score ΣFj*Wi</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>1.1.1 The policies for IT area are not documented</td>
<td>F1 3, F2 2, F3 3</td>
<td>2.65</td>
</tr>
<tr>
<td></td>
<td>1.1.2 The policies do not establish the responsibilities</td>
<td>F1 2, F2 3, F3 3</td>
<td>2.25</td>
</tr>
<tr>
<td></td>
<td>1.1.3 Employees do not know the policies that should be applied</td>
<td>F1 2, F2 3, F3 3</td>
<td>2.25</td>
</tr>
<tr>
<td></td>
<td>1.1.4 Policies are not updated</td>
<td>F1 2, F2 2, F3 2</td>
<td>2</td>
</tr>
<tr>
<td>1.2</td>
<td>1.2.1 Missing long term strategy</td>
<td>F1 2, F2 2, F3 2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1.2.2 Missing short term strategy</td>
<td>F1 1, F2 3, F3 2</td>
<td>1.95</td>
</tr>
<tr>
<td></td>
<td>1.2.3 Lack of correlation between the short and long term strategy</td>
<td>F1 2, F2 2, F3 2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1.2.4 Lack of correlation between the targets set in the strategy</td>
<td>F1 1, F2 3, F3 2</td>
<td>1.95</td>
</tr>
</tbody>
</table>

2 Questionnaire approach

Controls testing are performed through audit procedures which will follow two main issues [3]:

a) assess the design effectiveness of internal controls;
b) operability evaluation of internal controls.

Audit procedures that address the effectiveness of the design of internal controls, evaluates if those controls are properly established to prevent vulnerabilities of IT systems. Audit procedures aimed on efficiency review focuses to determine how controls were applied, the consistency with which they were applied and who implemented those controls. In addition to questions addressed to qualified staff and observation of the controls operation when testing the controls, the IT auditor must be able to restore the controls operations from the evidence gathered.

In order to conduct the audit, audit questionnaire will be developed to address all risks identified on the areas and subareas to be audited. Evaluation of risk coverage by controls will be based on responses received to questionnaires that include the control design and the operability evaluation through testing procedures.

The testing will be applied in all the situations where samples can be provided. The sample will be 15% of the population but no more than 20 records.

For the significant risks identified during introduction we have developed the following questionnaire:

<table>
<thead>
<tr>
<th>Significant Risk Addressed</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1</td>
<td>IT policies are documented?</td>
</tr>
<tr>
<td>1.1.1</td>
<td>IT policies have been approved by the organization management?</td>
</tr>
<tr>
<td>1.1.2</td>
<td>The policies contain clearly defined objectives and the measures required to be implemented?</td>
</tr>
<tr>
<td>1.1.2</td>
<td>Management structures are defined to administer and monitor the achieving objectives?</td>
</tr>
<tr>
<td>1.1.3</td>
<td>There is a process by which employees become aware of IT policies and their changes?</td>
</tr>
<tr>
<td>1.1.4</td>
<td>Policies are regularly updated?</td>
</tr>
</tbody>
</table>
1.2.1 A strategic plan on long term is developed and includes IT considerations?

1.2.1 There are strategies developed by each department that support the strategic plan?

1.2.1 The strategic plan covers all the processes taking place within the organization?

1.2.1 The strategic plan was approved by the organization management?

1.2.2 The activities undertaken by short term strategy serve achieving the long term strategic plan?

1.2.3 The strategy contains correlation of the timeline for the established goals achievement?

1.2.4 A short term strategic plan is developed?

1.2.4 There is a process defined for monitoring the status strategic objectives achievement, and regular updates are presented to the management?

1.2.5 Resources are identified and allocated to each objective included in the strategy?

The questioner has two answers for each question: affirmative/negative.

### 3 Implication on the audit steps

In order to perform the audit, the following audit steps will be followed:

1. Employees training
2. Questionnaire completion
3. Results computation
4. Ration analysis
5. Nonconformities identification
6. Defining remediation plan
7. Nonconformities reevaluation

#### 3.1 Employees training

A training approach should be developed to assist employees in questionnaire completion, and the documentation that should be prepared to support the questionnaire. All affected employees should have the opportunity to attend the training sessions. Also during the training session, the audit scope and mission will be presented to the employees, for a better understanding [4].

#### 3.2 Questionnaire completion

The questionnaire with all the areas and subareas to be audited will be divided based on the client organization structure in order to be sent to the appropriate client personnel form completion. Also the questionnaire will be sent to each application administrator and server administrator, in order to cover the entire IT environment that was included in scope.

### 3.3 Results computation

After completing the questionnaire, we can calculate the residual aggregated risk, as the risk that was not reduced by effective controls.

In order for a risk to be covered by efficient controls it is necessary that all the questions allocated to that control to be answered affirmative.

After that we calculate the residual aggregated risk for each auditable activity by using the following formula [1]:

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

where:
- \( R_i \) - score for the risks that are not covered by efficient controls;
- \( R_j \) - score for each risk;
- \( i \) - total number of risks covered by efficient controls;
- \( j \) - total number of significant risks;
- \( k \) - total number of auditable activities;
- \( AR_k \) - residual aggregated risk for \( k \) activity.

Next step is to compute the total residual aggregated risk by using the following formula:

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

where:
- \( AR_k \) - residual aggregated risk for \( k \) activity;
- \( k \) - total number of auditable activities;
- \( R \) - total residual aggregated risk.

#### 3.4 Ration analysis

After computation is performed we can perform the ration analysis. The criteria that have to be met in order to give a favorable opinion are:
- all high risk (score over 2.3) should be covered by effective controls;
- the residual aggregated risk for each activity must not exceed a threshold of 0.3;
- the total residual aggregated risk must not exceed a threshold of 0.2.
The results obtained after ration analysis are discussed with the audit client in order to ensure that all the data have been processed and the results reflect the actual status of the client. Due to the high risk of questionnaire miss interpretation, great attention must be given to the result communication.

3.5 Nonconformities identification
Starting from the questionnaires completed we establish all the areas that have negative answers, and prepare the nonconformities list. The presentation of the nonconformities list to the client will include the area affected by insufficient control and the impact of this situation on the client activity.

3.6 Defining remediation plan
The list with all the nonconformities identified will be discussed with the client in order to establish a remediation plan with clearly defined implementation terms, resource allocation and responsibilities.

The remediation plan has to be feasible in order to be able to reduce the list of nonconformities identified to an acceptable level until the reevaluation is performed.

3.7 Nonconformities reevaluation
For the risks not covered by effective controls during the first phase of the audit, the following steps will be performed:
   a) perform a new reassessment of risks covered by ineffective controls;
   b) check the existence of compensating controls that could mitigate the risk.

This process is repeated, usually, until it we consider that more compensatory controls cannot be found, or the residual aggregated risk meets the established threshold.

4 Model implementation
We have implemented the model through a web based application. The user first step is to classify the organization audited, based on the tolerance to the IT system availability.

The second step for the user is to start completing the questionnaire by selecting the audit area.

After all the audit areas have been answered, the auditor will perform the result computation and will present the issues identified to the client.

In order to simplify the interaction with the application in the situation were the questionnaire is sent to different employees for completion, an option has been created for answers import.

The main issues encountered by using this model are: difficulties to obtain client agreement to implement mandatory controls in his organization due to current economic conditions; a significant period of time is spent to decide the remediation plan that will be implemented, due to the limited resources available; difficulties to find compensatory controls for the areas were during the testing, some items from the population selected for testing was ineffective.
5 Conclusions
The proposed model has the advantage that it can be applied to any type of organization and the disadvantage that it requires a large database of questions to cover the key areas of an IT audit. The necessity of such a model is given by the practical aspects resulting from an implementation in reducing the audit mission duration.

References: