# Key Components and Operability Evaluation of Internal Controls for Risk Assessment Modeling in IT Audit

CRISTIAN AMANCEI, TRĂIAN SURCEL
Economic Informatics Department
Academy of Economic Studies
Bucharest
ROMANIA
cristian.amancei@ie.ase.ro, tsurcel@ase.ro

*Abstract:* the purpose of this paper is to present some directions to improve the implementation methodology of an audit process, from the analysis of tolerance to IT systems unavailability for organizations in a critical situation caused by the materialization of IT vulnerabilities. The article follows a series of key components of IT risk management process, proposing practical elements for risk control, internal controls operability analysis and aggregation of results, providing a deterministic model process. The use of predefined questionnaires and risk matrix can help the services providers to adapt to the market and maintain the service quality. These practical elements can be found in the proposed IT audit questionnaire, along with a workflow process in seven steps for the audit mission.

*Key-Words:* IT systems tolerance, risk areas and subareas, control evaluation, risk assessment, IT risk, IT audit steps, audit questionnaires

## 1. Introduction

The key components of the risk management process, as they are defined in the main methodologies [11], [12] are presented in figure 1.

### 1.1 Risk assessment

For the risk assessment, the following will be performed: impact assessment of the information commercial value; assessing the level of threat as a measure of the probability if there is a deliberate attack or an accidental event and establish the commercial impact that might result if the threat is manifested; assessing the vulnerability as a process of identifying, quantifying and ranking the vulnerabilities in the system; assessing the risk by combining the impact of threat and vulnerability, if there is a potentially high impact and high level of threat and vulnerability, then there is a high risk to the business.

### 1.2 Controlling risk

Involves taking steps to address the assessed risks, which involve actions into several forms: from risk avoidance to risk reevaluation as shown in figure 1.

### 1.3 Risk reporting

This documentary deals with processes and reporting risks. Risks are documented in a form agreed and communicated to those responsible in the context of risk reporting.

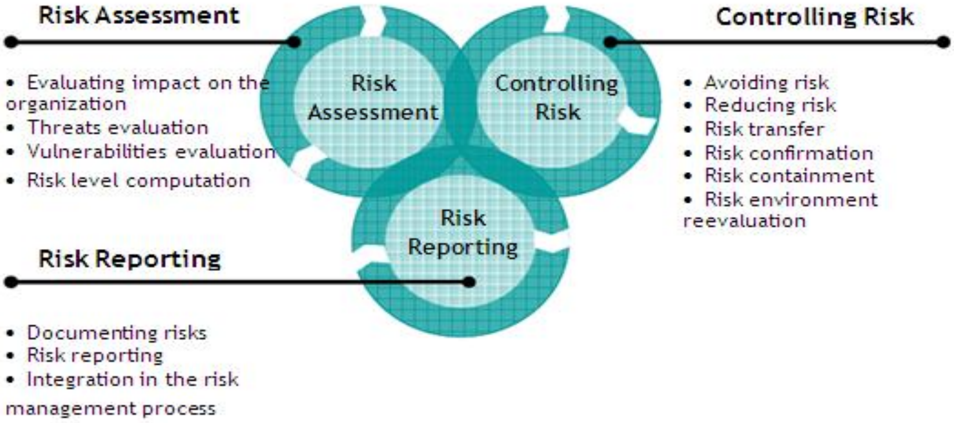


*Fig. 1: Key components of risk management process*

## 2. IT systems tolerance and significant risks evaluation

The approach presented in this paper, that uses the implications of using organizations tolerance to the IT systems unavailability in audit risk assessment, 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 by using the levels defined in table 1.

| Category | Tolerance to the IT systems unavailability |
|---|---|
| Organizations with critical IT systems | <2 working days |
| Organizations with medium IT systems | 2-4 working days |
| Organizations with uncritical IT systems | >4 working days |

*Table 1: Categories of tolerance to IT systems unavailability*

Given the existence of a correlation at the organization level, between the availability of systems and the budget and resources allocated for IT operations, that will have a direct impact on the control environment developed in the organization, it is necessary that the composition of the audit areas to be linked to IT department resources.

Due to this reason, and the fact that any organization will not invest in developing a control environment to mitigate the risks identified, if the future benefits expected will not considerable exceed the investment made, a structure of areas and subareas to be audited for each organization category has been developed, as presented in the table below:

| Area | Subarea to be audited | Category | | |
|---|---|---|---|---|
| | | Critical | Medium | Uncritical |
| 1. IT strategic plan | 1.1 Organization policies in IT area | X | X | X |
| | 1.2 Short term IT strategy | X | X | X |
| | 1.3 Long term IT strategy | X | X | |
| | 1.4 IT budget | X | X | |
| | 1.5 The information systems used for the main functions of the organization | X | X | X |
| | 1.6 The integration of information systems used | X | X | |
| | 1.7 Performance indicators for IT department | X | | |
| 2. IT department organization | 2.1 IT department organization chart | X | X | X |
| | 2.2 Job description for each position in the IT department | X | X | X |
| | 2.3 Employees qualification and trainings, including continuous training | X | X | X |
| | 2.4 Employee performance evaluation system | X | | |
| | 2.5 Segregation of duties in IT department | X | X | |

*Table 2: Areas and subareas to be audited for each organization category*

The audit approach begins with the Corporate IT Risk Management framework, which should be a holistic and structured approach that aligns governance policies, business strategy, management procedures, business processes and operational activities with the purpose of evaluating and managing risk and uncertainties the organization faces [8], [9].

The main objective this framework model is to align IT resources, IT infrastructure, key resources (data, people, assets, etc.) and business processes with governance policies and management procedures in order to effectively manage IT risk exposure [10].

The two fundamental groups of methods applied for analysis of risk on which assets are exposed in enterprises are quantitative and qualitative methods presented below [5]:

- quantitative, where estimation of risk value is connected with application of numerical measures – value of resources is defined in amounts, the frequency of threat occurrence in the number of cases, and susceptibility by the value of probability of its loss, those methods present results in the shape of indicators. The examples of quantitative methods: Annual Loss Expected, Courtney's and Fisher's methods, ISRAM model, etc.
- qualitative, which do not operate on numerical data, presenting results in the form of descriptions, recommendations, where

risk assessment risk is connected with: qualitative description of assets' value, determination of qualitative scales for the frequency of threat occurrence and susceptibility for a given threat or description of so called threat scenarios by prediction of the main risk factors. The examples of qualitative methods: FMEA/FMECA, The Microsoft Corporate Security Group Risk Management Framework, NIST SP 800-30, CRAMM.

Starting from these methods, we have decided to apply a combined risk approach, by using the following key risk factors during risk assessment [2]:

- 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 3.

| Risk factors ($F_i$) | Risk factors weights ($W_i$) | Level of risk assessment ($L_i$) | | |
|---|---|---|---|---|
| | | $L_1$ | $L_2$ | $L_3$ |
| Internal control assessment F1 | $W_1$ - 40% | There are procedures and are applied | There are procedures but are not applied | Procedures do not exists |
| Quantitative assessment F2 | $W_2$ - 35% | Low financial impact | Medium financial impact | High financial impact |
| Qualitative assessment F3 | $W_3$ - 25% | Low vulnerability | Medium vulnerability | High vulnerability |

*Table 3: Levels of risk factors*

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.

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 [11], [12], an example being presented in the table below:

| Subarea to be audited | Significant risks | Criteria for risk analysis | | | Total score |
|---|---|---|---|---|---|
| | | **F1** | **F2** | **F3** | **$\Sigma F_i * W_i$** |
| 1.1 | 1.1.1 The policies for IT area are not documented | 3 | 2 | 3 | 2.65 |
| | 1.1.2 The policies do not establish the responsibilities | 2 | 2 | 3 | 2.25 |
| | 1.1.3 Employees do not know the policies that should be applied | 2 | 2 | 3 | 2.25 |
| | 1.1.4 Policies are not updated | 2 | 2 | 2 | 2 |
| 1.2 | 1.2.1 Missing long term strategy | 2 | 2 | 2 | 2 |
| | 1.2.2 Missing short term strategy | 1 | 3 | 2 | 1.95 |
| | 1.2.3 Lack of correlation between the short and long term strategy | 2 | 2 | 2 | 2 |
| | 1.2.4 Lack of correlation between the targets set in the strategy | 1 | 3 | 2 | 1.95 |
| | 1.2.5 Necessary resources are not allocated | 1 | 3 | 3 | 2.2 |
| 2.4 | 2.4.1 Performance criteria are not clearly defined | 3 | 1 | 2 | 2.05 |
| | 2.4.2 Objectives are not clearly defined | 2 | 2 | 2 | 2 |
| | 2.4.3 Annual performance evaluation was not conducted / completed | 1 | 2 | 2 | 1.6 |
| | 2.4.4 Career development plan has been prepared | 2 | 2 | 1 | 1.75 |

*Table 4: Total score for significant risks*

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.

This risk classification has been applied on table 4.

## 3. Risk management process for information security

The risk management process for information security is developed for use across the organization. This process is very important for the organization stakeholders that can gain trust from proper management of the risk exposure.

The process is divided into four major sections:

1. Entry points in risk assessment method
2. Risk assessment process for information security
3. Risk confirmation process
4. Corporate risk management

### 3.1 Entry points in risk assessment method

In this section are listed the events that determine the risk assessment performance. These are the main factors that can trigger the risk management process [13].

### 3.2 Risk assessment process for information security

This section describes the risk assessment process. The process begins by defining the objective evaluation and planning of the entire review process. Detailed analysis of threats and vulnerabilities is the next step performed in this section. After that the analysis of how the risks will be addressed is performed, by ensuring the selection of checks that will ensure the selection of a perfect relationship between costs and risks mitigation. The last step is to document the outcomes and, if necessary, reporting is initiated.

### 3.3 Risk confirmation process

If it is not possible to identify in time reduction measures for the risks issues, the risk confirmation process is initiated. Through this process risks will be confirmed and reviewed to establish appropriate control measures that the organization can implement [3].

### 3.4 Corporate risk management

If the risks identified during the assessment exceed an established threshold, the risks must be reported to the management level specialized in corporate risk assessment. The threshold is defined for each unit / process within the company.

## 4. Questionnaire approach

Controls testing are performed through audit procedures which will follow two main issues [1]:

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

After performing these audit procedures, the auditor has to evaluate the quality of a business process models used by the client organization through a set of quality metrics. One specific category of metrics is coupling, which measures the functional and informational dependencies between the tasks/processes in a business process model, as proposed in [7].

Audit procedures that are addresses 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 30 records. The testing will address the controls efficiency, in order to evaluate the risks mitigated by those controls. The population selection for the control efficiency evaluation is very important in order to determine if the control was efficient through the entire audit period.

A representative sample is one in which the characteristics in the sample of audit interest are approximately the same as those of the population. The manner in which the population is filed or distributed will determine the kind of selection techniques to be used to select the sample.

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

| Significant Risk Addressed | Questions |
|---|---|
| 1.1.1 | IT policies are documented? |
| 1.1.1 | IT policies have been approved by the organization management? |
| 1.1.2 | The policies contain clearly defined objectives and the measures required to be implemented? |
| 1.1.2 | Management structures are defined to administer and monitor the achieving objectives? |
| 1.1.2 | All the employees responsible for implementing the policies are aware of the approved framework? |
| 1.1.3 | There is a process by which employees become aware of IT policies and their changes? |
| 1.1.3 | Is the employee's awareness tested performed periodically? |
| 1.1.4 | Policies are regularly updated? |
| 1.1.4 | All the updates have followed the approval process? |
| 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? |
| 1.2.2 | The short term strategy includes IT considerations? |
| 1.2.2 | The short term strategy has been approved by the organization management? |
| 1.2.3 | The strategy contains correlation of the timeline for the established goals achievement? |
| 1.2.3 | The management involvement in achieving the objectives is correlated between the two strategies? |
| 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? |
| 1.2.5 | Resources allocation conflicts has been identified and resolved? |
| 1.2.5 | Resources allocate are aware of their future involvement? |
| 2.4.1 | The performance criteria are clearly defined and measured during the performance management process? |
| 2.4.1 | Performance criteria awareness programs are conducted inside the organization? |
| 2.4.2 | Objectives are established for each position in the organization? |
| 2.4.2 | Clear measurement methods for the objectives established are defined? |
| 2.4.2 | The measurement methods are agreed with the organization employees? |
| 2.4.3 | Was the annual performance evaluation performed during last year? |
| 2.4.3 | The results of the performance evaluation are communicated in the organization along with the proposed action plans? |
| 2.4.4 | Each employee has a career development plan defined and analyzed during the performance evaluation? |
| 2.4.4 | Career development plan are aligned with the future skills needed by the organization? |

*Table 5: Questioner for significant risks*

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

## 5. 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

### 5.1 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].

### 5.2 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. This questionnaire is designed to address the effectiveness of internal controls defined in the client organization.

### 5.3 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:

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

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.

### 5.4 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 reflects the actual status of the client control environment.

Due to the high risk of questionnaire miss interpretation, great attention must be given to the result communication.

### 5.5 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.

### 5.6 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.

### 5.7 Nonconformities reevaluation

For the risks not covered by effective controls during the first phase of the audit, the following steps will be performed:

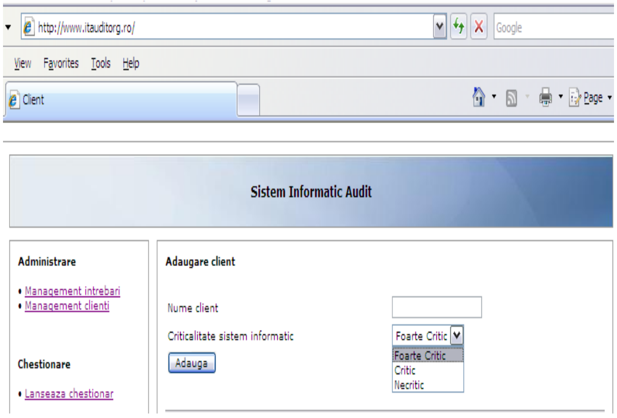
a) perform a new reassessment of risks covered by ineffective controls;
b) check the existence of compensating controls that could mitigate the risk.

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.

## 6. 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 unavailability, figure 2.



Sistem Informatic Audit

Administrare

- Management intrebari
- Management clienti

Chestionare

- Lanseaza chestionar

Adaugare client

Nume client

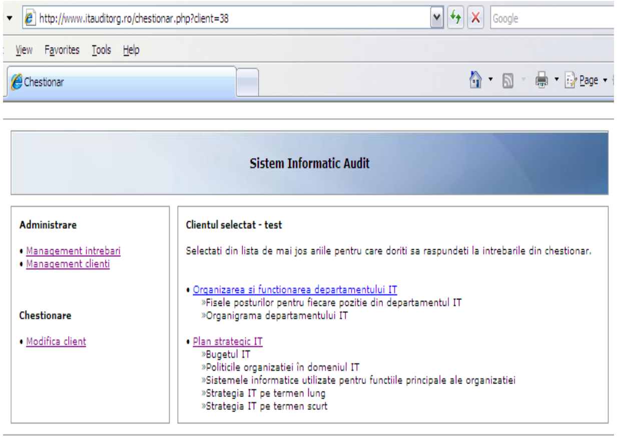
Criticalitate sistem informatic: Foarte Critic

Foarte Critic
Critic
Necritic

Adauga

Fig. 2: Client classification

The second step for the user is to start completing the questionnaire by selecting the audit area, figure 3.


http://www.itauditorg.ro/chestionar.php?client=38
Google
View Favorites Tools Help
Chestionar
Page

Sistem Informatic Audit

Administrare

- Management intrebari
- Management clienti

Chestionare

- Modifica client

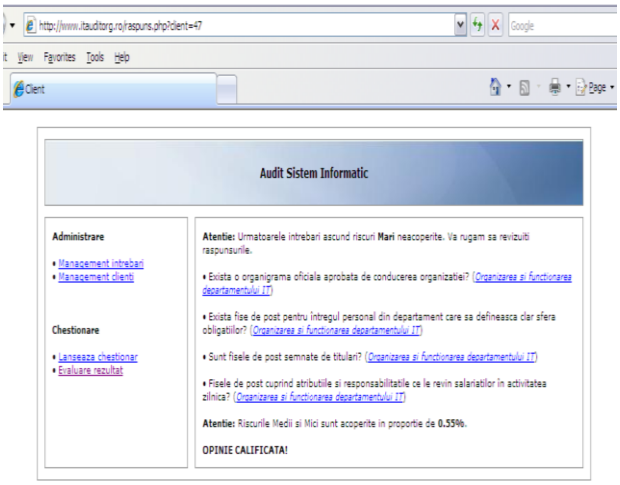
Clientul selectat - test

Selectati din lista de mai jos ariile pentru care doriti sa raspundeti la intrebarile din chestionar.

- Organizarea si functionarea departamentului IT
  »Fisele posturilor pentru fiecare pozitie din departamentul IT
  »Organigrama departamentului IT
- Plan strategic IT
  »Bugetul IT
  »Politicile organizatiei în domeniul IT
  »Sistemele informatice utilizate pentru functiile principale ale organizatiei
  »Strategia IT pe termen lung
  »Strategia IT pe termen scurt

Fig. 3: Questionnaire audit areas selection

After all the audit areas have been answered, the auditor will perform the result computation, as in figure 4, and will present the issues identified to the client.


http://www.itauditorg.ro/raspuns.php?client=47
Google
View Favorites Tools Help
Client
Page

Audit Sistem Informatic

Administrare

- Management intrebari
- Management clienti

Chestionare

- Lanseaza chestionar
- Evaluare rezultat

**Atentie:** Urmatoarele intrebari ascund riscuri **Mari** neacoperite. Va rugam sa revizuiti raspunsurile.

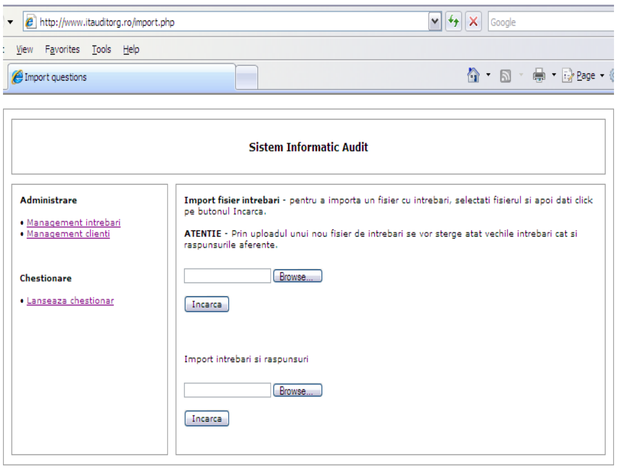
- Exista o organigrama oficiala aprobata de conducerea organizatiei? (*Organizarea si functionarea departamentului IT*)
- Exista fise de post pentru întregul personal din departament care sa defineasca clar sfera obligatiilor? (*Organizarea si functionarea departamentului IT*)
- Sunt fisele de post semnate de titulari? (*Organizarea si functionarea departamentului IT*)
- Fisele de post cuprind atributiile si responsabilitatile ce le revin salariatilor în activitatea zilnica? (*Organizarea si functionarea departamentului IT*)

**Atentie:** Riscurile Medii si Mici sunt acoperite in proportie de **0.55%**.

**OPINIE CALIFICATA!**

Fig. 4: Audit results evaluation

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, presented in figure 5.


http://www.itauditorg.ro/import.php
Google
View Favorites Tools Help
Import questions
Page

Sistem Informatic Audit

Administrare

- Management intrebari
- Management clienti

Chestionare

- Lanseaza chestionar

**Import fisier intrebari** - pentru a importa un fisier cu intrebari, selectati fisierul si apoi dati click pe butonul Incarca.

**ATENTIE** - Prin uploadul unui nou fisier de intrebari se vor sterge atat vechile intrebari cat si raspunsurile aferente.

Browse...

Incarca

Import intrebari si raspunsuri

Browse...

Incarca

Fig. 5: Questionnaire 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 were ineffective.

## 7. Operability evaluations of internal controls

The auditor tests controls by reviewing the history of documentation that connects the transactions/operations to the client's records. The sample of transactions/operations selected for testing depends on the control type: manual, IT dependant, application control. Normally, for application controls, 12 transactions are to be tested. One transaction is selected from each month to ensure that the application control operates effectively throughout the year. For IT dependant application controls a larger population of transactions will be selected (2-3 transactions from each month).

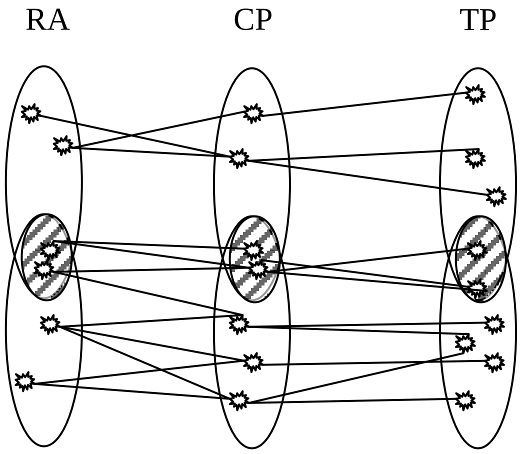
If the auditor encounters an error in control testing, they will first consider whether the error is systematic or isolated. Systematic errors normally have a pervasive impact on the control system, so the auditor will not be able to rely on controls unless a compensating control is identified and tested. If the error is isolated, the auditor will expand their testing sample by adding 30-40% transactions. If the larger sample size does not yield any additional errors, the control system is considered effective.

During the audit mission, the auditor has to decide the testing procedures that will be applied for the selected risk areas that will be inspected. The complexity of the control environment is represented in figure 5. In this complex environment the auditor decision has to be efficient and rapid.

Usually this analysis is performed for each type of control (manual, IT dependant, application control) due to the implications that the controls testing sample has on the audit mission duration. The auditor will try to identify application controls that address the selected risks, after that will search for IT dependant controls and at the end will look for manual controls.

The sample size has a big impact on the time allocated for control testing. The bigger the sample size is the more time will be spend on gathering the audit evidence.

For selecting the testing procedures that will be applied for each control type, the auditor will use the φ (optimum control procedures) and β (optimum testing procedures) functions.



where:
RA - risk areas;
CP - control procedures;
TP - testing procedures.

*Fig. 6: Relationship between risk areas, control procedures and testing procedures*

As we can see represented in figure 6, the relationship between risk areas, control procedures and testing procedures is many too many.

In order to increase the efficiency of the resource utilization during audit mission, the auditor will identify the risks that are at the risk areas diagrams crossing and after that the control procedures and testing procedures that address the selected risk. The selection of control procedures and testing procedures will be performed by using as a criterion, the number of links with the risk areas and control procedures.

To perform this implementation, the auditor will associate weights for each control procedures and testing procedures by analyzing their position in the risk environment (if is placed in the crossing area or not) and the number of links of each selected element.

The sum of weights for each control procedure and testing procedure diagram will be constant, to ensure the comparability of the results. Each auditor will define his own weights allocation values, depending on the above mentioned criteria, and will ensure the consistency of the method selected.

The auditor will apply the φ and β functions in order to identify the testing procedures that will be applied during the field work phase of the audit mission.

$$\varphi : (RA_i \cap RA_j) \to \lambda(CPW_k) \Rightarrow \{CPW_k^*\} \quad (3)$$

where:
RA - risk areas;
CPW - control procedures weight;
$CPW^*$- selected control procedures based on the above criteria.

$$\beta : (CP_i \cap CP_j) \to \mu(TPW_k) \Rightarrow \{TPW_k^*\} \quad (4)$$

where:
CP - control procedures;
TPW - testing procedures weight;
$TPW^*$- selected testing procedures based on the above criteria.

The β function used for optimum testing procedure, will have as an input the control procedures diagrams previously identified.

The model efficiency will depend on the auditor ability to establish correct weights for control procedures and testing procedures.

Beside the selection of the testing procedure, the selection of the sampling plans is very important for the results that can be obtained from the audit mission.

The further increase the capabilities of these models, continuous auditing model should be approached. There are studies that propose the uses of Web services technology to support auditing processes, such as [6]. In these studies, the continuous auditing functionality is defined as a set of Web services that reside within the auditee's computer system rather than the auditor's system. The next generation of audit missions should relay on continuous auditing models.

## 8. Conclusions

The proposed model has the advantage that I can be applied to any type of organization and the disadvantage that it requires a large database o 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.

Future research could look at the automatic audit practices and discuss the new risks that have to be introduced in the proposed model, in order to provide on-demand data and real-time assurance. Based on our study, we consider that further research should include business process models evaluation through a set of quality metrics.

The cost effectiveness of audit mission is more critical than ever, and will bring the society benefits, so the research of risk assessment in IT audit implementation is valuable to our society.

*References:*

[1] I. Ivan, G. Noşca and S. Capisizu, *Informatics Systems Audit*, ASE Publishing House, Bucharest, 2005

[2] Ghita M., *Internal Audit second edition*, Economics Printing House, Bucharest, 2009

[3] F. Lyons, *Auditing Change* Controls, IT Audit & Controls 28th Annual Conference, MIS Training Institute's, Las Vegas, 2008

[4] S. Senft, F. Gallegos, *Information Technology Control and Audit*, third edition, Auerbach Publication, 2009

[5] A. Rot, *Enterprise Information Technology Security: Risk Management Perspective*, Proceedings of the World Congress on Engineering and Computer Science 2009, Vol II, 2009, pp. 1171-1176

[6] Huanzhuo Ye, Yuning He, *A Continuous Auditing Model Based on Web Services*, 7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science, Hangzhou, China, 2008, pp. 406-411

[7] W. Khlif, N. Zaaboub, H. Ben-Abdallah, *Coupling metrics for business process modeling*, WSEAS Transactions on Computers, Issue 1, Vol. 9, 2010, pp. 31-41

[8] 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

[9] N. Azizi, K. Hashim, *Enterprise Level IT Risk Management*, Proceedings of the 8th WSEAS Int. Conf. on Applied Computer Science, 2008, pp. 401-404

[10] N. A. Panayiotou, S. P. Gayialis, T. A. Panayiotou, V. I. N. Leopoulos, *Risk Management Issues in the Implementation of an ERP System for a Large Greek Company*, WSEAS Transactions on Computers, Issue 4, Vol. 3, 2004, pp. 1005-1012

[11] IT Governance Institute, "*CobiT 4.1, Framework – Control Objectives – Management Guidelines – Maturity Models*", 2007

[12] International Standard "*ISO/IEC 27001, Information Technology – Security Techniques – Information Security Management Systems – Requirements*", First Edition, 2005

[13] R. E. Cascarino, *Auditor's Guide to Information System Auditing*, John Wiley Printing House, Bucharest, 2007