Increasing the Efficiency of IT Audit Methodology by Using the Organizations Tolerance to IT Systems Availability

Cristian AMANCEI, Traian SURCEL
Bucharest Academy of Economic Studies
cristian.amancei@ie.ase.ro, tsurcel@ase.ro

The purpose of this paper is to present a method of identifying key risks during IT audit of an organization, regardless of the organization activity, and presenting the impact of the risks identified on the audit methodology. Our main focus is reducing the risk identification during phase during an audit mission. Due to the fast changing economy, the need for efficiency in resources allocation is greater than ever. Optimal use of predefined risk matrix proves to be the main element contributing to an increase in efficiency.
Keywords: *Audit, Risk Assessment, Audit Areas, Residual Aggregated Risk*

1 Introduction

Following the analysis of control practices in IT area (such as ITIL, COBIT, ISO27001 [8], [9], [10]) developed by renowned organizations in the field, we propose carrying out the IT audit based on a methodology that uses the following steps:

1. organizations tolerance to the IT systems availability;
2. identification of areas and subareas to be audited;
3. risk factors and associated weights;
4. the level, the total score and the ranking of significant risks;
5. conduct audit procedures based on questionnaires and testing;
6. residual aggregated risk assessment.

2 Organizations tolerance to the IT systems availability

One of the most important efficiency indicators of a computer system is the response time, which is the time interval between the request launch and the moment when it receives the response to the request issued. Response time is determined both on functional components such as queries, but also on complex components to the level of subsystem and information system. If the response time exceeds a well established limit, then serious failures occur that could compromise the conduct of business. The maximum permissible limit by which the organization can operate without the support of the information system is the level of availability.

The first step in performing the IT audit within an organization is, to establish the level of service availability that the IT department needs to ensure within the organization. The level is established based on: the organization profile, the support offered by the IT department in achieving the organization's main activities (e.g. production, sales or office support), the importance of assets held by the IT department.

Based on these criteria, we establish the category that fits the organization and its IT system, table 1.

Table 1. Organizations classification based on the tolerance to the IT systems availability

Category	Tolerance to the IT systems availability
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

3 Identification of areas and subareas to be audited

The tolerance level of the organization regarding the availability of the IT systems has direct implications on the resources assigned to IT. As the organization's tolerance to the availability of IT systems increases, the level of resources allocated to this department decreases [6].

Given the existence of this 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 [5], table 2.

Table 2. List of areas and subareas to be audited by organization category

Area	Subarea to be audited	Category		
		Critical	Medium	Uncritical
I. IT strategic plan	Organization policies in IT area	X	X	X
	Short term IT strategy	X	X	X
	Long term IT strategy	X	X	
	IT budget	X	X	
	The information systems used for the main functions of the organization	X	X	X
	The integration of information systems used	X	X	
	Performance indicators for IT department	X		
II. Organization and operation of IT department	IT department organization chart	X	X	X
	Job description for each position in the IT department	X	X	X
	The skills and the training of the employees, including continuous training in the field	X	X	X
	Employee performance evaluation system	X		
	Segregation of the activities for the IT department	X	X	
III. IT systems	Procedures for access to IT systems management, application change management, and incidents handling	X	X	X
	Detailed network diagram	X	X	
	Network diagram			X
	Hardware and network architecture	X		
	User guide and owners manuals	X	X	
	Licenses situation	X	X	X
	Training users of IT systems	X	X	X
	The monitoring of the privileged users access	X		
	Controls over correct processing in applications	X	X	
	Contracts with suppliers	X	X	X
	Monitoring and evaluating the service level	X	X	
IV. IT security	Procedures for IT security	X	X	X
	Monitoring implementation of IT security policy and procedures	X	X	
	Physical controls in IT	X	X	X
	Information classification	X		
	Security of network access and data communicated over the network	X	X	
	Antivirus and firewall	X	X	X
	Backup management	X	X	X
	Business continuity plan	X		
	Disaster recovery plan		X	

4 Risk factors and associated weights

General methodological rules recommended for risk analysis using three risk factors or criteria, which covers the activities audited, namely [1] [3]:

- 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. We mention that the sum of risk factors weights must be 100.

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, based on the model presented in table 3.

Table 3. Establishing risk factors, weights and levels of risk assessment

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

The risk factors considered are generic risk factors that cover any entity, but they can be customized if the situation encountered in customer demands. Thus, the list may be supplemented with other risk factors, such as: recent changes in the systems used; the likelihood of fraud by using IT systems [4].

5 The level, the total score and the ranking of significant risks

To establish the risk level we have used a scale of values with three levels for the three risk factors mentioned above: internal control assessment (F1); quantitative assessment (F2); qualitative assessment (F3). In this stage 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 [7].

In preparing this analysis were considered best practices, applied to an organization that has a tolerance to the availability of IT systems less than 2 days. 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 four categories of activities to be audited: IT strategic plan, organization and operation of IT department, IT systems and IT security, and auditable subareas within each class, we consider appropriate to analyze them by using the criteria (risk factors) and establish a total score for the following risks which we have inventoried, presented in the table 1.

Table 4. Areas, subareas to audited, significant risks and total score

No.	**Area**	**Subarea to be audited**	**Significant risks**	**Criteria for risk analysis**			**Total score ΣF_i*W_i**	**Classification**
				F1	**F2**	**F3**		
1	IT strategic plan	Organization policies in IT area	The policies for IT area are not documented	3	2	3	2.65	HIGH
			The policies do not establish the responsibilities	2	2	3	2.25	MEDIUM
			Employees do not know the policies that should be applied	2	2	3	2.25	MEDIUM
			Policies are not updated	2	2	2	2	MEDIUM
		Short term and long term IT strategy	Missing long term strategy	2	2	2	2	MEDIUM
			Missing short term strategy	1	3	2	1.95	MEDIUM
			Lack of correlation between the short and long term strategy	2	2	2	2	MEDIUM
			Lack of correlation between the targets set in the strategy	1	3	2	1.95	MEDIUM
			Necessary resources are not allocated	1	3	3	2.2	MEDIUM
		IT budget	Lack of correlation between the budget and the short and long term strategy	1	3	2	1.95	MEDIUM

			Allocation of poor resources for projects approved	1	3	2	1.95	MEDIUM
		The information systems used for the main functions of the organization	Main functions are not covered with appropriate information systems	2	3	2	2.35	HIGH
			Lack of tracking for system development/modification	2	2	3	2.25	MEDIUM
			Necessary resources are not allocated	1	3	3	2.2	MEDIUM
		The integration of information systems used	Procedures for interface/transfers between systems monitoring are not documented	3	3	3	3	HIGH
			Lack of interface/transfers between systems monitoring	2	2	3	2.25	MEDIUM
			Incidents occurred during the monitoring are not analyzed to identify and eliminate the caused that led to their occurrence	2	2	3	2.25	MEDIUM
		Performance indicators for IT department	Lack of performance indicators for IT department	3	2	3	2.65	HIGH
			Lack of performance indicators monitoring	1	2	2	1.6	LOW
			Measures are not implemented to comply with agreed indicators level	2	2	2	2	MEDIUM
2	Organization and operation of IT department	IT department organization chart	Department organization chart is not approved	3	2	3	2.65	HIGH
			Department organization chart is not updates/complete	2	2	2	2	MEDIUM
		Job description for each position in the IT department	Job descriptions are not signed by the holders	3	3	3	3	HIGH
			Job description does not include positions filled during holidays by addressing the segregation of duties	2	2	3	2.25	MEDIUM
		The skills and the training of the employees, including continuous training in the field	Continuous training plan has not been prepared and approved	3	2	2	2.4	HIGH
			Continuous training plan was not met	1	2	2	1.6	LOW
			Lack of documents attesting continuous training of staff	2	2	2	2	MEDIUM
		Employee performance evaluation system	Performance criteria are not clearly defined	3	1	2	2.05	MEDIUM
			The objectives are not clearly defined	2	2	2	2	MEDIUM
			Annual performance evaluation was no carried out/completed	1	2	2	1.6	LOW
			Career development plan has not been prepared	2	2	1	1.75	MEDIUM
		Segregation of the activities for the IT department	Lack of segregation of duties in the execution of operations by operational procedures requirements	3	3	3	3	HIGH
			Lack of incompatible operation knowledge	2	2	2	2	MEDIUM
			Lack of monitoring of compliance to procedures that ensures separation of activities	1	2	3	1.85	MEDIUM
3	IT systems	Procedures for access to IT systems management,	Lack of procedures for access to IT systems management, application change management, and incidents handling	3	3	3	3	HIGH

		application change management, and incidents handling	Procedures for access to IT systems management, application change management, and incidents handling are not updated and approved	3	2	2	2.4	HIGH
			Lack of monitoring on the procedures used for access to IT systems management, application change management, and incidents handling, and analysis of the results	2	2	3	2.25	MEDIUM
		Detailed network diagram	Detailed network diagram is not developed	3	2	3	2.65	HIGH
			Network diagram is not updated	2	2	2	2	MEDIUM
		Hardware and network architecture	Hardware and network architecture is not developed	3	2	3	2.65	HIGH
			Lack of update for hardware and network architecture	2	2	2	2	MEDIUM
		User guide and owners manuals	Lack of user guide and owners manuals	3	3	3	3	HIGH
			Lack of manuals completeness verification by key systems users	2	1	2	1.65	LOW
		Licenses situation	Lack of monitoring on the number of licenses acquired in relation to the number of existing users, for each application	2	3	3	2.6	HIGH
		Training users of IT systems	Lack of users training for IT systems (new IT systems or new functionality)	2	3	3	2.6	HIGH
			Lack of testing for the minimum knowledge needed	2	2	2	2	MEDIUM
		The monitoring of the privileged users access	Lack of procedures for monitoring privileged user's access (administrators, supers user etc.)	3	3	3	3	HIGH
			Missing evaluation of the activities performed in the system by privileged users by trained personnel	2	2	3	2.25	MEDIUM
		Controls over correct processing in applications	Lack of proper controls for each application correct processing (validation/control totals/cross-checking etc.)	3	3	3	3	HIGH
			Lack of monitoring over the controls for correct processing, and lack of action plans to correct errors arise	2	2	3	2.25	MEDIUM
		Contracts with suppliers, including monitoring and evaluating the service level	Lack of contract data expiration/extensions monitoring for the service suppliers	1	3	3	2.2	MEDIUM
			Missing service level evaluation for each contract	2	2	2	2	MEDIUM
4	IT security	Procedures for IT security	Lack of procedures for IT security	3	3	3	3	HIGH
			Procedures for IT security are not updated and approved	2	2	2	2	MEDIUM
			Employees do not know the procedures for IT security that should be applied	2	2	2	2	MEDIUM
		Monitoring implementation of IT security policy and procedures	The processed for IT security monitoring are not defined	3	3	3	3	HIGH
			Incident monitoring list is incomplete	2	2	3	2.25	MEDIUM
			Incidents occurred during the monitoring are not analyzed to identify and eliminate the caused that led to their occurrence	2	2	2	2	MEDIUM

		Physical controls in IT	Lack of physical controls in IT (restricted access to important equipment, systems, ventilation/air conditioning, fire systems, warning systems against unauthorized access/fire etc.)	3	3	3	3	HIGH
			Lack of maintenance/periodic verification of physical controls	2	2	2	2	MEDIUM
		Information classification	Lack of procedures for information classification	3	3	3	3	HIGH
			Information classification procedures are not updated and approved	2	2	2	2	MEDIUM
			Lack of monitoring of information classification within the organization	1	3	3	2.2	MEDIUM
		Security of network access and data communicated over the network	Users are not trained on the use of the computers network and its security	3	3	3	3	HIGH
			Network configuration standards are not documented	3	2	3	2.65	HIGH
			Criteria for monitoring network traffic are not established	3	2	3	2.65	HIGH
			Data is not recorded and kept unaltered for all key events occurred in the network	2	2	3	2.25	MEDIUM
			Sensitive data traffic is not defined and encrypted	3	3	3	3	HIGH
			Alternative channels for data traffic are not provided	2	2	2	2	MEDIUM
		Antivirus and firewall	Lack of procedures for antivirus and firewall configuration	3	3	3	3	HIGH
			Configuration procedures are not updated and approved	2	2	3	2.25	MEDIUM
			Lack of monitoring of antivirus and firewall applications	1	3	2	1.95	MEDIUM
		Backup management	Procedures data backup are not documented	3	3	3	3	HIGH
			The backup is not stored in a safe place or in another location	1	2	3	1.85	MEDIUM
			The media type used are not periodically reviewed to determine whether stored data can be read	2	2	3	2.25	MEDIUM
		Business continuity plan	Business continuity plan is not documented	3	3	3	3	HIGH
			The procedures to be followed in the business continuity plan are not complete or are know by the key employees	2	3	3	2.6	HIGH
			Business continuity plan is not tested	2	2	3	2.25	MEDIUM
			Backup system does not allow restoration of the activity during the critical time interval	2	2	3	2.25	MEDIUM

6 Conduct audit procedures based on questionnaires and testing

Controls testing are performed through audit procedures which will follow two main issues [2]:

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

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 and the results of testing the audit 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.

7 Residual aggregated risk assessment

After testing the controls by applying the above methods, we can calculate the residual aggregated risk, as the *risk that was not reduced by effective controls*. For the risks not covered by effective controls, the following steps will be performed:

a) check the existence of compensating controls or the possibility to implement new automatic controls;
b) perform a new reassessment of risks covered by ineffective controls.

This process is repeated, usually, until it we consider that more compensatory controls cannot be found, or the residual aggregated risk is insignificant.
We will first 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 - total score for the risks that are not covered by efficient controls;
R_j - total 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.
We will calculate 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.
After that we can assess the audit result. In order to give a favorable opinion, it is required that all high risk (score over 2.3) should be covered by effective controls and the total residual aggregated risk does no exceed a threshold of 0.3.

8 Conclusions

The advantage presented by developing a methodology for the classification of organizations, identifying and evaluating a minimum list of significant risk, becomes relevant when the audit is performed. This approach leads to reducing the time allocated for the audit engagement, having available a minimum list of significant risks, and the auditor's involvement in the audit mission will not be diminished, his main role being to review if necessary, the level of risk, and to introduce other risks identified in order to improve the methodology.

References

[1] M. Ghita, *Auditul intern editia a doua*, Economica Printing House, Bucharest, 2009.
[2] I. Ivan, G. Noşca and S. Capisizu, *Auditul sistemelor informatice*, ASE Publishing House, Bucharest, 2005.
[3] M. Staron, W. Meding, C. Nilsson, "A framework for developing measurement systems and its industrial evaluation," *Information and Software Technology Journal*, Vol. 51, 2009, pp. 721-737.
[4] T. Surcel and C. Amancei, "The IT Audit – A Major Requirement for the Quality Management and Success in the European Business Context," *The International Scientific Conference*, Oradea, 2008.
[5] M. Popa, F. Alecu and C. Amancei, "Characteristics of the Audit Process for Information Systems", in *Proc. The Proceedings of the International Conference Competitiveness and European Integration – Business Information Systems & Collaborative Support Systems in Business*, Cluj-Napoca, October 26 – 27, 2007, Risoprint Printing House, Cluj-Napoca, pp. 295 – 299.
[6] P. Panda, "The OCTAVE® Approach to Information Security Risk Assessment," *Information Systems Control Journal*, Vol. 4, 2009, pp. 37-42.
[7] S. Schlarman, "IT Risk Exploration: The IT Risk Management Taxonomy and

Evolution," *Information Systems Control Journal*, Vol. 3, 2009, pp 27-31.
[8] IT Governance Institute, *CobiT 4.1, Framework – Control Objectives – Management Guidelines – Maturity Models*, 2007.
[9] *International Standard ISO/IEC 27001, Information Technology – Security Techniques – Information Security Management Systems – Requirements*, First Edition, 2005
[10] *International Standard ISO/IEC 27002, Information Technology – Security Techniques – Code of Practice for Information Security Management*, Second Edition, 2005.

Cristian AMANCEI is University Assistant at Academy of Economics Studies Bucharest, Faculty of Economic Cybernetics, Statistics and Informatics. He is a PhD candidate from October 2007 at Economic Informatics Department from Academy of Economic Studies. He holds a Master in Science – Computerized Project Management from Academy of Economic Studies, Bucharest. He is Certified Information Systems Auditor (CISA). He graduated in Economic Informatics at Faculty of Economic Cybernetics, Statistics and Informatics in 2006. His main research areas are: information system audit, data structures, metrics in information systems and object oriented programming.

Traian SURCEL is Professor at Academy of Economic Studies Bucharest, Faculty of Economic Cybernetics, Statistics and Informatics, Department of Informatics in Economy, PhD in Economic Cybernetics from 1987. He coordinates the Fundamentals of IT&C for Business Management professors group and also PC Laboratories for Faculty of, Marketing, Commerce and International Business and Economics. Hi is Internal Auditor for the ASE Bucharest. His main research areas are: information system and database analyze and design, IT systems audit, e-Learning applied methodology, IT&C for Business Management.