Dávid PETŐ

KNOWLEDGE REUSE IN CREATING AUDIT PLANS

In this research the question of knowledge reusability in creating more reliable IT audit plans has been investigated. With the use of appropriate simulation techniques and statistical analysis, it has been proved that the explicit usage of self-reflection in IT auditing enables more precise audit plans, therefore the execution might become more effective. This self-reflection means that auditing methodologies are largely depending on the results of previous examinations of certain areas. In fact, the most widespread methods and guidelines are also based on the experience gained through previous examinations. If the results gathered in this way are being used, more precise audit plans can be made and the designation of the areas to be examined can become more accurate. If the fact that audit methodologies are primarily based on practical experience is accepted and explicitly formulated, then, with the use of the information acquired in previous audits, better and more precise audit plans can be created. In other phrases: the assignment of control objectives in certain situations of examination can be done based on the experiences from previous audits. Additionally, the audit plans created in this way enable the cost-effective execution of audits, without sacrificing accuracy and reliability. The results of the simulation confirm these statements.

Keywords: **IT audit, methods, risk control**

The purpose of IT audit reports is to inform the company's executives of the revealed situation, let them know of the possible deficiencies, and preferably to offer ways of solution. Obviously though, the decisions have to be made by the executives themselves.

It is a common and serious problem that managers are not provided with all the necessary information to make their decisions regarding information technology issues. This is true in spite of the fact that audit reports present a description of the areas with higher risks, the risk factors in these fields and often the possible solutions as well. Audit reports do not help in the decision which areas the limited resources should be invested in for effective treatment. Decision-makers often make the allocation of different resources in an *ad hoc* manner to cure the diverse problems. In their decision, they mainly rely on their previous experiences.

Another problem, although its cause is basically the same, is that the results achieved by different audit processes, especially the ones regarding risk levels, are not comparable with each other. As there is no commonly agreed regulation for the assessment of risks, the evaluation is usually made in a highly subjective manner (Ozier, 2003). Thus, even if numerical indices are available concerning certain areas, they cannot be compared to other cases, as another auditor might reach different results, even if the method and the investigated problems are the same. The risk levels in the results of different audits made in different periods in the same organization, or different companies in the same industry, are not comparable.

According to the assumption made in this research a metrics that is based on a widespread methodology and that secures more precise measurement and comparability of different risks, helps in optimizing corporate resource-allocation in the areas involved, and – thanks to this and the benchmarking capabilities – enhancing the efficiency, numerical representation and verifiability of company decisions based on the audit results.

An additional achievement is that by calculating the risk levels more precisely the results of previous audit processes can be used to more accurately delimit the areas of interest. Therefore auditing knowledge

might be reused in order to make more specific audit plans. This paper describes the steps taken to verify this assumption and also its consequences regarding knowledge reusability.

The usability of knowledge in auditing

The goals of auditing

The main goal of an information technology audit, similarly to other methods of supervision, is to examine compliance. Thus, to check whether the processes, control and operation of the inspected areas comply with some kind of predefined regulations. Therefore, there are only two kinds of results of an audit process: complying or not complying.

The intention in regulating corporate operation is to restrain the different operational risks in order to achieve the strategic goals. Obviously to make compliance measurable in a suitable way, controls must be built into the company's processes. In our case these are derived from the Control Objectives of COBIT, the methodology that has been used as a basis for the research.

But the question that is one of the key issues of this research arises: to what extent does the appropriate selection of controls (control objectives) enhance risk reduction? Do the appropriate narrowing down of the area of focus or the amount of questions that have to be examined result in the cost-effective reduction of risks derived from corporate IT? If the knowledge gained in previous audits is used to articulate the self-reflection of the assessment system, does it help in selecting the right control objectives?

Audit plans based on previous experiences

We might presume that the use of risk assessment metrics during IT auditing contributes to the optimization of the allocation of corporate resources. Executives responsible for IT governance are in a difficult position when they have to decide on countermeasures against risks (Trites, 2004). Without an appropriate measurement method it is hard to precisely determine the desirable use of resources. The metrics creates a chance to make optimal decisions on the use of resources.

Our assumption was that if the self-reflecting nature of the execution of IT audits is formulated explicitly, the results can be reused to improve and more accurately specify the audit plans.

Information technology audit is essentially based on previous experiences. Most methodologies (including ITIL, Common Criteria, COSO ERM and also COBIT) are actually a collection of best practices (ITIL, 1989; CC, 1999; COSO, 2004). Therefore, the data from different audits is obviously worth to be used to more precisely define the assessment method. According to our assumption, the refinement can be carried out if the results of previous audits are used in an appropriate way.

Risk assessment metrics as a tool for knowledge reuse

The primary goal of this research was the creation of a risk assessment metrics based on a widely spread methodology, which might be used in information technology auditing, and optionally the creation of a software system that might be of use in the audit process by providing support for the auditors. After the appropriate methodological funding and the choice of methods, the research has been mainly of practical nature, as on basis of the principal background, the assessment method was constructed, as well as the scaling and the tool that provides the necessary support for the users.

There were several prerequisites of the research. First, a comprehensive collection of the possible risks had to be created that could be used as the foundation of the assessment. Second, the appropriate measurement and ranking method had to be shaped, namely the metrics that is capable of the evaluation of the risk factors and the totalling on certain areas.

As the goal was to create a method that can be used in many areas, the definition of risks also had to be as wide as possible. To reach this goal an audit methodology had to be selected that is both widespread and detailed enough so the certain risks could be generated with its use in a direct or indirect way.

There is only one comprehensive audit methodology that fulfils the above criteria, which is accepted by most experts, covers the most possible areas, but at the same time is suitable for the deconstruction so the risk factors can be reached. This is the COBIT methodology, issued by ITGI and ISACA (COBIT, 2000). Although there has been some criticism on the completeness of the threats to information integrity mentioned in COBIT (Boritz, 2005), this is obviously the methodology that covers most of the areas in question.

On the other hand, COBIT does not originally include such deconstruction that would allow the direct analysis of risks. Although it provides serious help in creating the control questions on risks, the extraction of actual risk factors from this standard needed further work.

The other task was the creation of the metrics itself. The method is described below.

To make the metrics functional, the calibration of the method had to be done. This was assured by the execution of several measurements and the recording and comparison of data. The operation of the index was tested with the use of Monte Carlo simulation.

Creating the index

The aim of the research has been to create a method that allows the certain determination of the risk level regarding the examined company; thus, the making of a risk index that defines the risk level, based on the data collected during the audits.

In order to reach this goal, the widely used guidelines of COBIT were used as a research basis. In its construction, COBIT (3rd edition) contains 34 control objectives grouped in four domains. The control objectives cover practices to follow that are important in the information security and effective operation of the company. As further specification, these contain more than 300 detailed control objectives, which are to specify and more precisely define the higher-level objectives. Although the 4th edition of COBIT has been published recently, the basic concept has not changed.

According to its objective, COBIT covers every area related to corporate information technology, therefore the risk factors may be considered as the most comprehensive possible. This is the reason why the detailed control objectives of COBIT were taken as a basis for the identification of risks in this research.

COBIT makes the evaluation of control objectives possible only by assigning levels of 1 to 5 (0 in the case of non-applicable) to them, based on the capability-maturity models. This results a variable that is measurable only on an ordinal scale that is not appropriate for calculating averages or other statistical indices. For the sake of easier usage, these evaluations can be taken into consideration in a way that the risk linked to the control objective raises or lowers the risk of the company (or some of its parts).

The main concept of the risk assessment method is the following: the auditor assigns the capability-maturity levels regarding the individual factors on the area in focus (There have been attempts to create metrics based on this concept (Jelen, 2000)). Relying on these the decision can be made whether the certain factor raises or lowers the risk level. As a starting point, the acceptance threshold, namely the line between raising and lowering is 2.5, which is only used as a parameter in the model. Based on these data, the risk level of the investigated area can be defined with the use of a certain algorithm.

The most straightforward algorithm is the calculation of a simple mean. In this case the values of +1 and -1 are added, which show the contribution to the risk level. Obviously, this method is not capable of supplying refined data and it is not useful in practice, as one cannot state the equal importance of all factors. With the use of this simple method, it is inevitable that such factors extinguish each other that are obviously of different importance in real life. With the use of a method like that, it is impossible to define the areas where the resources have to be concentrated upon, as all problems appear to be of same severity.

As a result the introduction of importance weights was also necessary. With this method, which appears in most of the known risk assessment tools as well, it is possible for the auditor to consider the different importances of the individual factors. There are several methods to assign the weights (Hwang – Shin – Han, 2004); the choice between these is not part of this research.

To use this method, the allocation of appropriate weights is also expected from the person carrying out the audit; thus, the creation of a weighted average can be done. In the research, the making of the weights can rely on the scenarios. Namely, during the examination such sets were defined that determine the areas to be analyzed in certain industries (e.g. banks, manufacturing etc.). The weights of the examined areas are also expected to be different in these cases.

Mapping the interactions

At the same time, the allocation of weights does not solve another important problem: the interaction of risk factors. During the research, the conclusion was drawn that the assessment of risks can be much more precise if the factors are not regarded independent, but their relationships are also taken into account.

To reach this goal the effects of the coexistence of two simultaneous factors had to be mapped. For example it could be defined how the overall risk index is going to be affected by the coexistence of the two factors when the quality of the plan on IT strategy is a factor raising the risks and the qualification of the personnel is a factor lowering the risks. Obviously, these estimations cannot be done in a totally faultless way. As there are no historical data on regarding these questions, expert estimations had to be relied on. At the same time this is not opposed to the viewpoint of COBIT, as this is a collection of empirical knowledge, therefore its individual statements are not unquestionable.

As a result of the detailed discovery work, an interaction matrix was created that contains these simultaneous effects *(see table 1).*

Table 1.

A section of the interaction matrix

domain_id	id	PO 1		PO 2		PO 3		PO 4		PO 5		PO 6		PO 7		PO 8		PO 9		PO 10		PO 11		AI 1		AI 2		AI 3		AI 4		AI 5		AI 6		DS 1	
PO	1			1	-1	1	0	1	1	1	-1	1	1	1	1	1	0	1	-1	1	-1	1	1	1	0	1	-1	1	-1	1	-1	1	1	1	-1	1	0
				1	-1	1	-1	1	-1	1	-1	-1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	0	-1	1	-1	1	-1	1	-1	-1	-1	1	-1	0	-1
PO	2					1	1	1	0	1	1	1	-1	1	-1	1	0	1	-1	1	1	1	-1	1	1	1	-1	1	-1	1	1	1	-1	1	0	1	1
						-1	-1	0	-1	-1	-1	-1	-1	0	-1	-1	-1	0	-1	-1	-1	0	-1	0	-1	1	-1	0	-1	-1	-1	1	-1	-1	-1	-1	-1
PO	3							1	-1	1	1	1	0	1	0	1	-1	1	-1	1	0	1	-1	1	-1	1	-1	1	-1	1	-1	1	0	1	0		
								1	-1	-1	-1	0	-1	0	-1	1	-1	1	-1	0	-1	0	-1	1	-1	1	-1	1	-1	0	-1	1	-1	0	-1	1	-1
PO	4									1	1	1	0	1	0	1	0	1	-1	1	0	1	0	1	0	1	-1	1	-1	1	-1	1	0	1	1	1	1
										-1	-1	-1	-1	-1	-1	-1	-1	1	-1	0	-1	0	-1	1	-1	1	-1	1	-1	0	-1	0	-1	-1	-1	-1	-1
PO	5											1	-1	1	-1	1	0	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	0	1	-1	1	1	1	-1
												1	-1	0	-1	0	-1	1	-1	1	-1	1	-1	0	-1	1	-1	1	-1	0	-1	1	-1	-1	-1	0	-1
PO	6													1	-1	1	-1	1	-1	1	0	1	-1	1	-1	1	-1	1	-1	1	0	1	-1	1	-1	1	1
														-1	-1	1	-1	1	-1	-1	-1	-1	-1	1	-1	1	-1	1	-1	-1	-1	-1	-1	1	-1	-1	-1
PO	7															1	0	1	-1	1	0	1	0	1	-1	1	0	1	0	1	1	1	-1	1	1	1	0
																-1	-1	1	-1	-1	-1	0	-1	0	-1	-1	-1	0	-1	-1	-1	0	-1	-1	-1	0	-1
PO	8																	1	-1	1	-1	1	-1	1	-1	1	-1	1	0	1	0	1	-1	1	-1	1	1
																		1	-1	0	-1	1	-1	1	-1	1	-1	0	-1	-1	-1	0	-1	0	-1	0	-1
PO	9																			1	1	1	1	1	0	1	0	1	0	1	0	1	1	1	1		
																				-1	-1	-1	-1	-1	-1	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
PO	10																					1	-1	1	-1	1	-1	1	-1	1	0	1	-1	1	1	1	1
																						0	-1	0	-1	1	-1	0	-1	0	-1	1	-1	-1	-1	0	-1
PO	11																							1	0	1	-1	1	-1	1	1	1	-1	1	1	1	-1
																								-1	-1	1	-1	1	-1	-1	-1	1	-1	-1	-1	1	-1
AI	1																									1	0	1	-1	1	-1	1	-1	1	1	1	1
																										0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1

On this basis, it was possible to develop the assessment procedure further. The determination of the risk index is done in such way that the capability-maturity indices and risk factors defined by the auditors are considered in selecting the certain elements of the matrix and the results are cumulated. The meaning of the certain squares of the matrix is made clear by table 2.

Table 2

Legend for the interaction matrix

		AI 1	
		+	-
PO 4	+	1	0
	-	1	-1

The upper left field shows the value that is appointed to the risk index when both factors in question perform in a positive way – in this case in the example, their coexistence lowers the overall risk (the positive number means the raising of security, therefore the lowering of risks). In the upper right field, the factor shown in the column on the left is positive and the one shown in the row on the top is negative. The other fields are also filled up according to the figure.

The algorithm of the index

By totalling and weighting the appropriate elements of the interaction matrix, the risk index can be created. The totalling can be carried out using the following formula:

$$R = \sum_{i=1}^{n} w_i \frac{r_i + \sum_{j=1}^{n} r_{i,j}}{n}, \text{ where } \sum_{i=1}^{n} w_i = 1$$

In which R is the overall risk index, wi is the weight of the certain risk factors, ri is the converted value of the risk index (-1or +1) and ri,j is the value created from the first-order interaction of the risk factors by the use of the above matrix (might be –1, 0 or +1).

Thus, the formula creates a weighted average of the risk indices including the interactions as well. The value ri is emphasized, as that is the direct contribution of the certain risk factor to the cumulated risk level. In fact this is the self-interaction of factor i, which is not else but its own risk value.

The benefit of the procedure is that the value of the index can be easily calculated for certain sub-domains as well, thus for the subset of overall risk consisting of some control objectives. The overall risk index then can be created by simply totalling these.

In case the auditor finds it hard to assign weights to certain areas with a total of 1, a transformation can be executed easily. Therefore it is possible to use practically any kinds of weighting, if the individual weights are divided by the total of weight values; namely, if the weights are normalized.

It might appear so that during the cumulating each risk interaction is considered twice, but this phenomenon is parried by the use of appropriate weighting. The attribution of weights is done according to the weights of parent-factors given by the auditor, and during the cumulating, the weights of individual risk factors (control objectives) are used.

The simulation experiment

Because of the lack of relevant data, Monte Carlo simulation was used during the research. The simulation and the generation of the results were carried out in several steps.

Scenarios

First, the formulation of 4 different scenarios took place, representing certain audit situations. Thus, the model of the examination of a bank, a manufacturer, a service company and a software development firm was created in such way that the detailed control objectives to be examined were identified depending on practical experience.

The importance of the creation of these scenarios regarding the goals of this research is that the different risk assessment methods may be distinguished from the aspect of their usability in diverse auditing situations. With the help of the scenarios, further peculiarities specific to the certain areas might be observed as well.

Random samples

Next, 500 random samples were created in order to represent the capability-maturity values defined in the auditing process. Equal distribution of the values was assumed when creating the random numbers, which means that each of the evaluation levels (measured on a scale of 0 to 5) had the same chance to be in the sample. Naturally, during further research, it is possible to change the distribution and make further analysis.

Random numbers were generated for the scenarios as well. In order to assure the comparability of the results, the same cases were used, thus each of the 500 cases used in the scenarios are shortlists of the random values created for the whole of the control objectives.

Conversion

In the next step the evaluations were transformed into the values +1 and –1, where +1 stands for the growth of security and –1 for its decrease, therefore the raising level of risks. There were two reasons to make this conversion: first, the values measured on an ordinal scale are obviously not usable directly to create numerical values – e.g. averages; second, the concept of the research was to make a separation of factors depending on whether they raise or decrease overall risk. Thus, the set of simulated data is divided in two groups depending on the acceptance threshold.

In the simulation, this threshold was 2.5, which is the middle of the range of values. As this is only a parameter of the model, this might be changed in further research. The threshold had been set at that level, as this made the enabled the allocation of equally distributed variables in two groups of the same size. However, if the distribution is changed, the shifting of the acceptance threshold might be needed. This is considerable also, because the value 0 is a special measure in the capability-maturity models, as this stands for not applicable.

Calculating the risk indices

The following step was the creation of the risk indices from the generated and transformed values. In order to do that, equally distributed weights had to be rendered to the factors, which were normalized to total 1. There are different weights attributed to each of the cases, therefore 500 different set of weights were used.

Four different indices were created in the research:

In the creation of the mean, simply the +1 and –1 values were averaged in each of the cases.

In the construction of the weighted average, the +1 and –1 values rendered to the control objectives were averaged with the use of the constructed weights.

In the index created with respect to the interactions, the respective elements of the interaction matrix (therefore the intersections rendered to the +1 and –1 values of the control objectives) are averaged.

Finally the creation of the R index, the goal of the research, was done. This index is created with respect ot the interactions and the different weights of the control objectives.

The calculation of the risk indices was made for each of the cases in the sample of 500 for all of the control objectives (thus, the risk factors), and also for the different scenarios. In this way, 500*5*4=10000 index values were created.

Statistical analysis

In the final step, the statistical analysis of the cumulated risk indices regarding the risk factors in the whole of the sample and also in each of the scenarios was made. With the help of these, it was possible to compare the different assessment methods concerning their basic attributes, and also the verification of the examined hypotheses. The statistical indices were created using SPSS software. The histograms illustrating the behaviour of the respective indices seriously support the analysis.

Results

The main results of the simulation experiment are the following: The average values of the indices created with respect to the interactions (the expected values of the variables) are shifted towards the negative values. This means that, by the use of the index suggested here, the risks of the organization in question might appear bigger than in the case of simple averaging. Namely, the shift towards the negative direction means that the value of the security index is lower. This is natural, and it reflects one of the main principles of auditing: prudence. This is the consequence of the fact that in cases where it was hard to decide on the effect of the interactions, negative values were preferred to be safe. This can also become clear by totalling the elements of the interaction matrix, as the result is a negative number.

The variation of the indices created with respect to interactions is higher than in the cases of simple averages. This additional variation calculated on basis of the matrix extended with fist- order interactions compared to the basic situation is generated by the simultaneous occurrence of risk factors. In this research, only the first-order relationships could be analysed. The additional variation generated by the second and higher order interactions could also be analysed one by one, but this is beyond the limitations of the present research. This is why Monte Carlo simulation had to be employed that allows the estimation of the effects of higher order interactions, therefore all further indirect impacts.

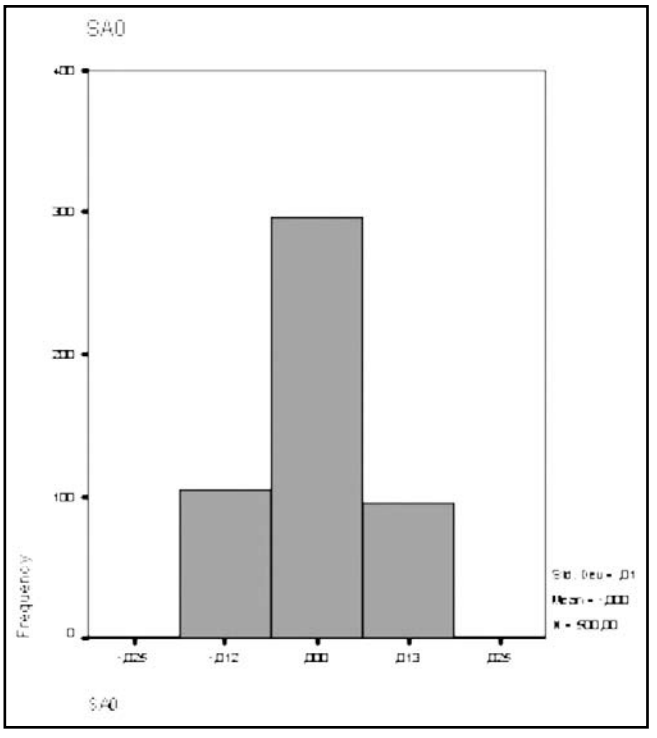
The operational strategy for moderation of risks and the goals of the IT function can be based on the intention to lower the additional variation discovered in the above-mentioned way. The importance of the method introduced in this paper is the capability of identifying such strategic focus points in addition to the explicitly formulated primary risks, which are impossible to discover without this approach.

By analysing the results of the simulation, the statement can be made that the positive or negative sign of the index considering the risk interaction is very seldom different from that of the simple average – only in cases with values close to 0. At the same time, the size of the shown risk might be considerably different, depending on the case. Thanks to this, the method is capable of raising the attention to special cases and orientate so that the simultaneous effects of the individual risk factors can be estimated.

While the use of weights lowers the variation in the case of the indices without respect of the interactions, variation is bigger in the indices considering the relationships compared to the not weighted methods. This method is capable of giving even more importance to the cases different from the usual, and raising the attention to hidden relationships (see Figure 1). Indirectly this verifies that there is a procedure that is capable of active management and articulation of hidden relationships. The weighting also expresses the relative importance and posed amount of threat by certain factors in certain moments.

Figure 1

The distribution of weighted averages in the sample containing all the control objectives

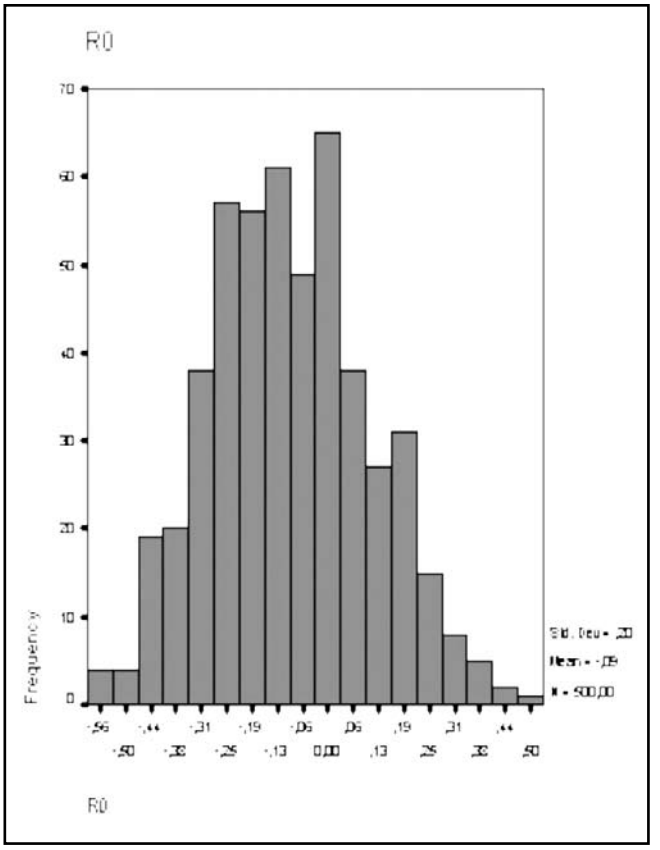


The range of the results – the distance of the minimum and maximum values – does not change, or gets larger with the insertion of interactions (also visible on the histograms). Therefore, the suggested method is creates the opportunity to raise attention to the cases differing from the average even more.

The effect of the weighting of risks is smaller than that of the consideration of the interactions. Thus, the difference in the totals of the weighted and not weighted cases is smaller, than the amount of the effects of taking the interaction in consideration.

Figure 2

The distribution of the R index in the sample containing all the control objectives



Comparing the suggested index and the simpler methods shows that the index considering the interactions as well is usually even more different in the examination of the scenarios than in the case of the whole of the control objectives. (Figure 2) This confirms that, if the amount of available information is less, the importance of this method is even bigger in determining the appropriate measure. In the case of the scenarios, the avoidance of individual risks is less important than the consideration of their simultaneous effects. With the use of the index that is the result of the research, the critical coexistences that influence corporate risk are easier to spot.

Thanks to the construction of the index, in the extreme cases (e.g. all factors are raising or all are lowering risk) there is no difference between the resulted values; at the same time in the cases in between, that are much more likely in real situations, the shift can be considerable.

Confirmation of the assumption

The practical meaning of our assumption is that if the fact that audit methodologies are primarily based on practical experience is used, then, with the use of the information acquired in previous audits, better and more precise audit plans can be created. In other phrases: the assignment of control objectives in certain situations of examination can be done based on the experiences of previous audits. Additionally, the audit plans created in this way enable the cost-effective execution of audits, without sacrificing accuracy and reliability. The results of the simulation confirm that the index created in the described manner is capable of the appropriate measurement of risks. As the creation of a risk index with the consideration of interactions succeeded; the self-reflecting quality of auditing was usable in creating the audit plan. Therefore our assumption is confirmed.

Knowledge reusability conclusions

As it is possible to create a cumulated risk index that considers the simultaneous effects of individual risk factors, a new method for the assessment of corporate risks is enabled. With the use of such metrics, previously unidentifiable risks can be brought into front. In some cases areas that remained hidden when using traditional methods, can now be considered of higher risk that need further investigation.

All this results in the possibility for corporate management to get a better and more accurate image of the information technology risk level of the organization. Because of the consideration of the relationships of risk factors, this suggested index is more capable of comprehensive assessment of larger areas, ranges consisting of more sources of risk in the company. This may be a tool in the hand of the management that allows the correction of strategy on a more objective basis.

It has become clear that the results of previous audits are usable in making more accurate and more purposeful audit plans. If the already examined areas and the relations on these are taken into consideration, it is possible to set up scenarios that employ the interactions of individual risk factors and their effects on overall risk. This also enables the more accurate designation of the critical areas regarding the examination. In this way, it is possible to create better audit plans that are easier to execute than previous ones.

If these data, the results of auditing, and their confirmation by indices are available, it becomes possible for corporate management to optimally distribute the resources related to information technology. The limited assets of the company can be used in such way, that IT risk management receives the most benefits possible.

It has to be noted, that the exploration of the results is not enough to realize the advantages mentioned above. In order that the executives be able to interpret the results, it is necessary to bring them to a format that is understandable for them; to "translate" these into the appropriate language. Therefore the tasks of the auditors do not end at creating the risk index. It is a further duty to put the results in an appropriate context, providing a handhold for corporate executives in the interpretation.

It has been confirmed that by employing the suggested index, the identification of such IT-related and strategically important areas is achievable that were indefinable with the use of traditional methods. This is primarily made possible by the fact that the consideration of joint effects of risk factors enables the perception of such co-existences that are important from the corporate strategy point of view, but which were impossible to discover due to the too few dimensions of risk indices.

References

Boritz, J. E. (2005): Is practitioners' views on core concepts of information integrity, International Journal of Accounting Information Systems, Vol. 6, Issue 4, pp. 260–279.

CC (1999): CSE-SCSSI-BSII-NLNCSA-CESG-NIST-NSA: Common Criteria for Information Technology security Evaluation

COBIT (2000): COBIT Framework, 3rd edition, IT Governance Institute, Rolling Meadows

COSO (2004): Enterprise Risk Management – Integrated Framework, Executive Summary, COSO, Jersey City

Hwang, S-S. – Shin, T. – Han, I. (2004): CRAS-CBR: Internal control risk assessment systems using case-based reasoning, Expert Systems, Vol. 21, Issue 1, pp. 22–33.

ITIL (1989): IT Infrastructure Library, Central Computer and Telecommunication Agency, London

Jelen, G. (2000): SSE-CMM Security Metrics, (online), NIST and CSSPAB Workshop, Washington, http://csrc.nist.gov./csspab/june13-15/jelen.pdf

Ozier, W. (2003): Risk metrics needed for IT security, IT Audit, Vol. 6.

Trites, G. (2004): Director responsibility for IT governance, International Journal of Accounting Information Systems, Vol. 5, Issue 2, pp. 89–99.

Cikk beérkezett: 2006. 12. hó
Lektori vélemény alapján átdolgozva: 2007. 3. hó

E SZÁMUNK SZERZŐI

Dr. Klimkó Gábor, vezető tanácsadó, MTA ITA, **Tóth Róbert,** informatikai tanácsadó, MOL Nyrt., **Dr. Fehér Péter,** egyetemi adjunktus, Budapesti Corvinus Egyetem, **Dr. Kő Andrea,** egyetemi docens, Budapesti Corvinus Egyetem, **Dr. Szabó Zoltán,** egyetemi adjunktus, Budapesti Corvinus Egyetem, **Pető Dávid,** tanársegéd, Budapesti Corvinus Egyetem, **Hajnal György,** PhD, tudományos főmunkatárs, Magyar Közigazgatási Intézet, **Dr. Borgulya Istvánné Vető Ágnes,** CSc, habilitált egyetemi docens, a közgazdaságtudomány kandidátusa, Pécsi Tudományegyetem, **Siklósi Árpád,** PhD. Hallgató, Budapesti Corvinus Egyetem, **Dr. Sascha Kraus,** assistant professor, University of Oldenburg, **Dr. Málovics Éva,** PhD, egyetemi docens, Szegedi Egyetem, **Rubóczky István,** nyugd. oszt. vez., **Dr. Osman Péter,** kandidátus, **Dr. Krisztián Béla,** egyetemi docens, Pécsi Tudományegyetem, **Dr. Véry Zoltán,** tudományos tanácsadó, IFUA