Audit of Virtual Systems Based on Vague Inputs Conducted by One or More Auditors

Jiří Bartoš, Cyril Klimeš
Department of Informatics and Computers
University of Ostrava
Ostrava, Czech Republic
{jiri.bartos, cyril.klimes}@osu.cz

ABSTRACT: *This article deals with the risk analysis and audits of virtual infrastructures. It gives a brief look into today's risk mitigation approaches and extends one with the evaluation of security by the evaluation based on linguistic variables with the expert system. The proposed methodology is able to cover audit process conducted by one or more auditors (users/ testers).*

Keywords: Audit, Security, Virtual System, Fuzzy, Risk Assessment

Received: 26 June 2013, Revised 29 July 2013, Accepted 3 August 2013

1. Introduction

Information systems and infrastructures are nowadays not only hardware systems with application software but also complex virtual infrastructures such as a virtual storage, virtual networks, virtual servers or even desktops. A proper risk analysis usually works with an asset cost, which can be very difficult to obtain (there is a difficulty to find the asset cost in a virtual environment, or even to find the asset itself). Also, the threat that affects the virtual environment could be (and often is) different than the one operating in a nonvirtual environment. Therefore, an approach to address the virtual infrastructure risk needs to be found.

Today's approach to measure the level of security of a virtual IT system can be divided into three major streams:

- The application of the best practices [8] or the definition of bad practices [10]
- The mitigation of the portion (portions) of the security domain [9]
- The evaluation based on strict and comprehensive guidelines [7]

2. Problem formulation

The first two approaches are strongly expert-required. That means that the auditor, the person that is conducting the security evaluation (or the risk analysis), needs to know every aspect of the *VM* technology and the risks associated with the virtual environment, as well as with the nonvirtual one (because of the transition from *hw* to *vm*) – basically, a virtual infrastructure architect is needed.

The third stream proposes the definition and the classification of security risks in virtual IT systems into three types with a deeper recognition of these types [7]:

• **Architectural vulnerability** — The layer of abstraction between the physical hardware and the virtualized systems running the IT services is a potential target of an attack. Just as the guest OS is subjected to the same security risks as a physical system, security measures (e.g., antivirus agents, spyware filters, IDs) should be installed on all VMs.

• **Software vulnerability** —The most important software in a virtual IT system is the hypervisor. Any security vulnerability in the hypervisor software will put VMs at risk of failure. The following steps are necessary as precautionary measures against software vulnerabilities:

• **Configuration risks** — Due to the ease of cloning and copying images, a new infrastructure can be deployed very easily in a virtual environment. This introduces a configuration drift; as a result, controlling and accounting for the rapidly deployed environments become a critical task.

Also this third stream proposes a set of guidelines that can be used as a questionnaire to cover the significant relevant areas to cover the virtual IT systems [7].

Unfortunately this approach does not remove the need for expert to the technology and its implementation, it only transfers some of the work to a simple analyst, or even the owner of the systems (in this context, the owner is defined as the person or group of people who have the responsibility for maintenance of the asset security [11]). This can be done and accomplished because of the guidelines, unfortunately, the expert is still needed for the evaluation and for the representation of the results, meaning, that the guidelines provide only limited evaluation, in terms of Yes/No answers (as shown in table 1) and are not linked to the security risks.

Risk Assessment		
Question	***YES***	***NO***
4. Is there a sufficient expertise to support the new environment?		
5. Has there been a sufficient training of the team for working and maintaining the virtual environment?		
6. Are the operational procedures regularly updated?		
7. Is there a single point of failure?		
8. Are the security zones separated or combined?		
9. How are the IT resources separated and aggregated in the VM environment?		
10. How is the VM environment security managed?		
11. Is there an administrative access to the host machine?		
12. Does the management console have a tight access controls, locked down to specific users and specific partitions or machines?		

Table 1. Filled questionnaire example containing only risk assessment

3. Problem solution

The guidelines are stray processes, but there is a problem with the lack of more meaningful or descriptive evaluations and therefore the problem lies in inadequate options and possibilities of questionnaire protocols and their assessment.

Therefore, the paper proposes an approach that will expend these guidelines with a better evaluation and representation of results and will incorporate the uncertainty in the assessment itself. In other words, the proposed approach will quantify the

qualitative assessment based on a vague description [2] of the results and the conformity of meeting the predefined criteria (security standard) [13].

The basis of the proposed approach is a fuzzy expert system that will not force the auditor (or the owner) to give an unambiguous quantification of the specific audit/assessment (or part), but will allow a vague (verbal) evaluation of the specific guideline (security area).

Also, it can be admitted that the owner [11] can be more than one person, so evaluation the audit inputs by more than one owner is allowed and, therefore, a better final assessment is produced.

The three above types of classification are obviously not enough, so they are furthermore developed from the point of which vulnerability they address, or what vulnerabilities they mitigate or to which they serve as precautionary [7] [14].

3.1 Methodology

As mentioned above, the proposed approach allows evaluation based on existing guidelines (it is using them and extending them). The results represent the level of the security conformance and the set of proposed countermeasures.

The proposed approach takes the guidelines [7] for automated processing of the vague results of their evaluation. The evaluation is than simply conducted by processing these vague results of audit with a fuzzy expert system [3]. So the results are smoother and the evaluation itself is not quantitative [6].

Visually, the proposed methodology is shown in Figure 1.

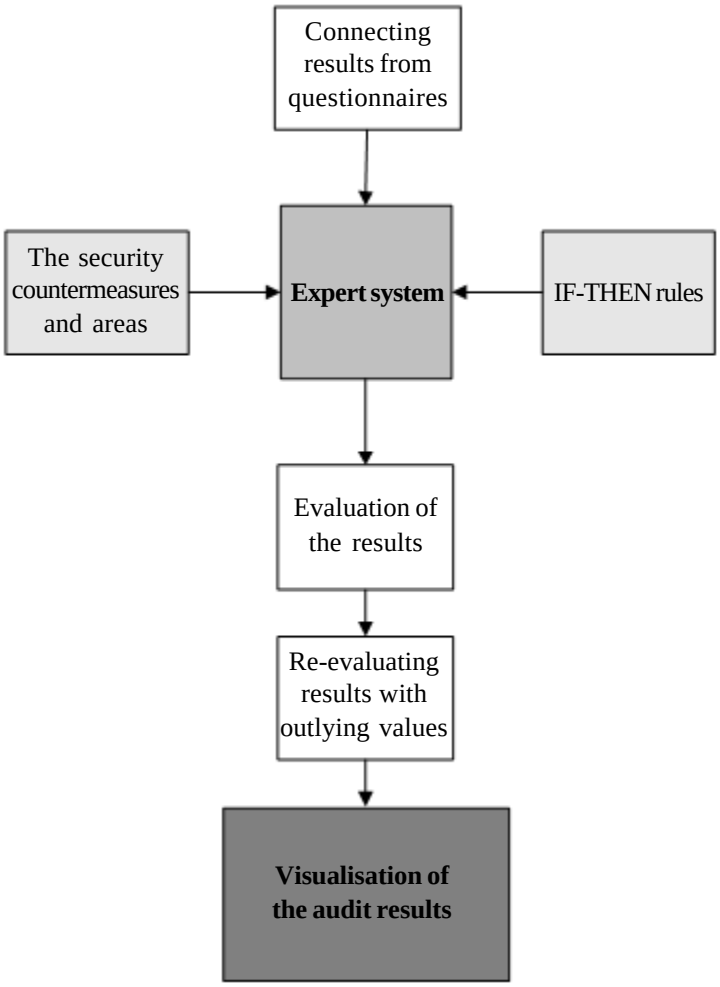

Figure 1. Proposed methodology

3.2 Creating a test questionnaire and collecting the test results

The questionnaire, together with the results of the owner (or individual owners), is shown in Table 2. For each criterion it is also necessary to define a set of outputs or values that may be used [1] by the tester during testing. For this work, the following set of values has been selected, which can be easily extended:

very small, *small*, *medium*, *big*, *very big*.

Risk Assessment	
Question	***Evaluation***
4. Is there a sufficient expertise to support the new environment?	Small
5. Has there been a sufficient training of the team for working and maintaining the virtual environment?	Very small
6. Are the operational procedures updated regularly?	Big
7. Is there a single point of failure?	Very big
8. Are the security zones separated or combined?	Very small
9. How are the IT resources separated and aggregated in the VM environment?	Medium
10. How is the VM environment security managed?	Small
11. Is there an administrative access to the host machine?	Small
12. Does the management console have tight access controls, locked down to specific users and specific partitions or machines?	Very Small

Table 2. Filled Questionnaire Example Containing Only Risk Assessment From Only One Owner

This questionnaire (or questionnaires) is collected and processed by the expert system. For that, an expert system knowledge base is built from [7] and [11] and can be (and is) extended. The knowledge base contains all criteria and sets of possible results on one hand and on the second hand the individual IF-THEN rules are composed from the input linguistic variables that correspond to each criterion and output linguistic variable and represent the expression [4] [5] of the evaluation of the audit.

For instance, this is how the "*Architectural vulnerability*" area is linked and extended (due to extensiveness of the knowledgebase, only a part of "*vulnerability analysis*" subsection is shown).

3.2.1 Vulnerability analysis

• 10.3.1 Capacity management

The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

• 10.3.2 System acceptance

Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during the development and prior to an acceptance.

• 10.10.1 Audit Logging

Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.

• 10.10.2 Monitoring system use

Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.

• 10.10.3 Protection of log information

Logging facilities and log information shall be protected against tampering and unauthorized access.

• 10.10.4 Administrator and operator logs
System administrator and system operator activities shall be logged.

• 10.10.5 Fault logging
Faults shall be logged, analyzed, and appropriate action taken.

• 15.2.1 Compliance with security policies and standards
Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

• 15.2.2 Technical compliance checking
Information systems shall be regularly checked for compliance with security implementation standards.

• 15.3.1 Information systems audit controls
Audit requirements and activities involving checks on operational systems shall be planned carefully and agreed to minimize the risk of disruptions to business processes.

• 15.3.2 Protection of information systems audit tools
Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

All the subsections (based on vulnerabilities they address, vulnerabilities they mitigate or to which they serve as precautionary) of all three areas:

For creating the knowledge base of the expert system, the LFLC tool can be used. This tool is able to define input and output linguistic variables and IF-THEN rules. The LFLC tool has also inference mechanisms and implemented defuzzification procedures, so a complete expert system can be created with this tool. The LFLC tool is more described in [19].

The IF-THEN rules are constructed over the questionnaire (or questionnaires in the case of multiple questionnaires) topics and are used for the evaluation conducted by the expert system:

*IF Q*11== *small AND Q*12 == *small THEN corresponding_countermeasures (a*1,*sa*4 == *small)*

*IF Q*7 == *small AND THEN corresponding_countermeasures (a*1, *sa*4 == *very small)*

*IF Q*8== *big AND Q*9 == *big THEN corresponding_countermeasures (a*1, *sa*1== *all)*

Where the set corresponding_countermeasures contains of two fields:

- a – area
- sa – subarea

where subarea value specifies the selected subarea and the expression furthermore specifies more detailed selection of the countermeasures and represents the effect of the countermeasure. The final decision made by the expert system is the process of the selection of the best variant of the proposed countermeasures, which is driven by the intersection of the proposed countermeasures from all the IF-THEN rules that were applied.

The evaluation of the single result (single owner) is a straightforward deffuzification process that is realized by the defuzzyfication of fuzzy sets, one of them is shown in the following picture (see Figure 2).

This deffuzification process transforms the vague evaluations into a percentage evaluation, where the upper and lower boundaries are represented by two extremes 0% and 100%.

When there is more than one owner, there are several evaluations on the input. The problem with multiple results of the expert system is their interpretation. Basically, the result of the processing is the percentage of the individual and afterwards overall evaluation of the audit. However, with multiple evaluations, the distribution of results is skewed and there can be intentionally or unintentionally manipulated audit results in the resulting set.

Architectural vulnerability	**Vulnerability analysis**	**Regular updates of sec. features on VMs**	**Proper management on VMs**	**Implementation of network best practices**
7.1.1 Inventory of Assets	**Medium**			
7.1.2 Ownership of assets	**Small**			
7.1.3 Acceptable use of assets	**Small**			
8.1.1 Roles and responsibilities	**Medium**	**Big**	**Big**	
9.2.2 Supporting utilities				**Small**
9.2.3 Cabling security				**Medium**
9.2.4 Equipment maintenance				**Medium**
10.3.1 Capacity management				**Big**
10.3.2 System acceptance				**Big**
10.6.1 Network controls				**Very big**
10.6.2 Security of network services				**Very big**
10.7.4 Security of system documentation				**Medium**
10.10.1 Audit Logging		**Small**	**Very small**	
10.10.2 Monitoring system use	**Small**	**Very big**	**Big**	**Medium**
10.10.3 Protection of log information	**Big**			
10.10.4 Administrator and operator logs		**Small**	**Very small**	
10.10.5 Fault logging	**Very big**			**Big**
10.10.6 Clock synchronization				**Medium**
11.1.1 Access control policy	**Big**			**Big**
11.4.1 Policy on use of network services				**Medium**
11.4.2 User authentication for external connections				**Very big**
11.4.3 Equipment identification in networks				**Small**
11.4.4 Remote diagnostic and configuration port protection				**Big**
11.4.5 Segregation in networks				**Very big**
11.4.6 Network connection control				**Very big**
11.4.7 Network routing control				**Big**
11.5.4 Use of system utilities			**medium**	**Medium**
11.5.5 Session time-out				**Small**
11.5.6 Limitation of connection time				**Small**
11.6.2 Sensitive system isolation				**Very big**
12.4.1 Control of operational software		**Small**	**Small**	
12.5.1 Change control procedures		**Small**	**Very small**	

Architectural vulnerability	Vulnerability analysis	Regular updates of sec. features on VMs	Proper management on VMs	Implementation of network best practices
12.5.2 Technical review of applications after operating system changes		**Medium**	**Small**	
12.5.3 Restrictions on changes to software packages	**Medium**			
12.6.1 Control of technical vulnerabilities	**Medium**			
13.1.1 Reporting information security events	**Medium**			
13.1.2 Reporting security weaknesses	**Medium**			
13.2.1 Responsibilities and procedures	**small**			
13.2.2 Learning from information security incidents Small				
13.2.3 Collection of evidence	**Medium**			
14.1.1 Including information security in the				
business continuity management process	**Very big**			
14.1.2 Business continuity and risk assessment	**Big**			
14.1.3 Developing and implementing continuity plans including information security	**Big**			
14.1.4 Business continuity planning framework	**Medium**			
14.1.5 Testing, maintaining and re-assessing business continuity plans	**Medium**			
15.2.1 Compliance with security policies and standards	**Small**			
15.2.2 Technical compliance checking				**Medium**
15.3.1 Information systems audit controls	**Very small**			
15.3.2 Protection of information systems audit tools	**Small**			

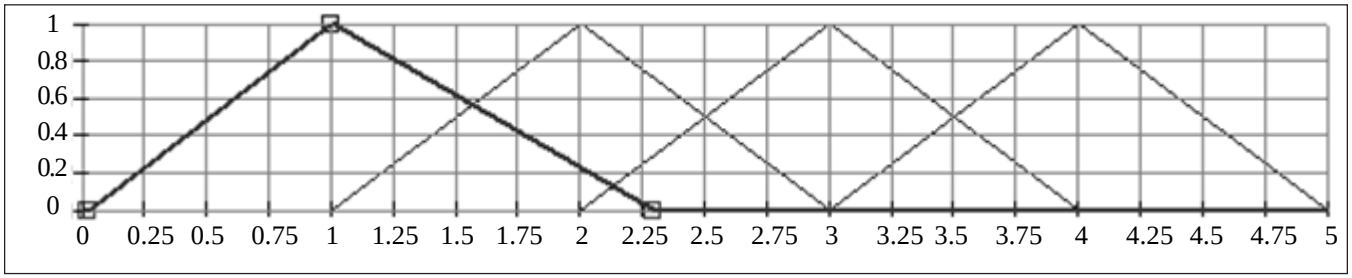

Figure 1. Form of fuzzy set corresponding to the evaluation and defuzzyfication of 4 input attributes

When the distribution is skewed, the mean is usually not in the middle so a median $\tilde{x}$ will be computed as the middle value in a set of results that needs to be ordered first. The computation is very simple: when there is an odd number of results, the middle median is computed simply as:

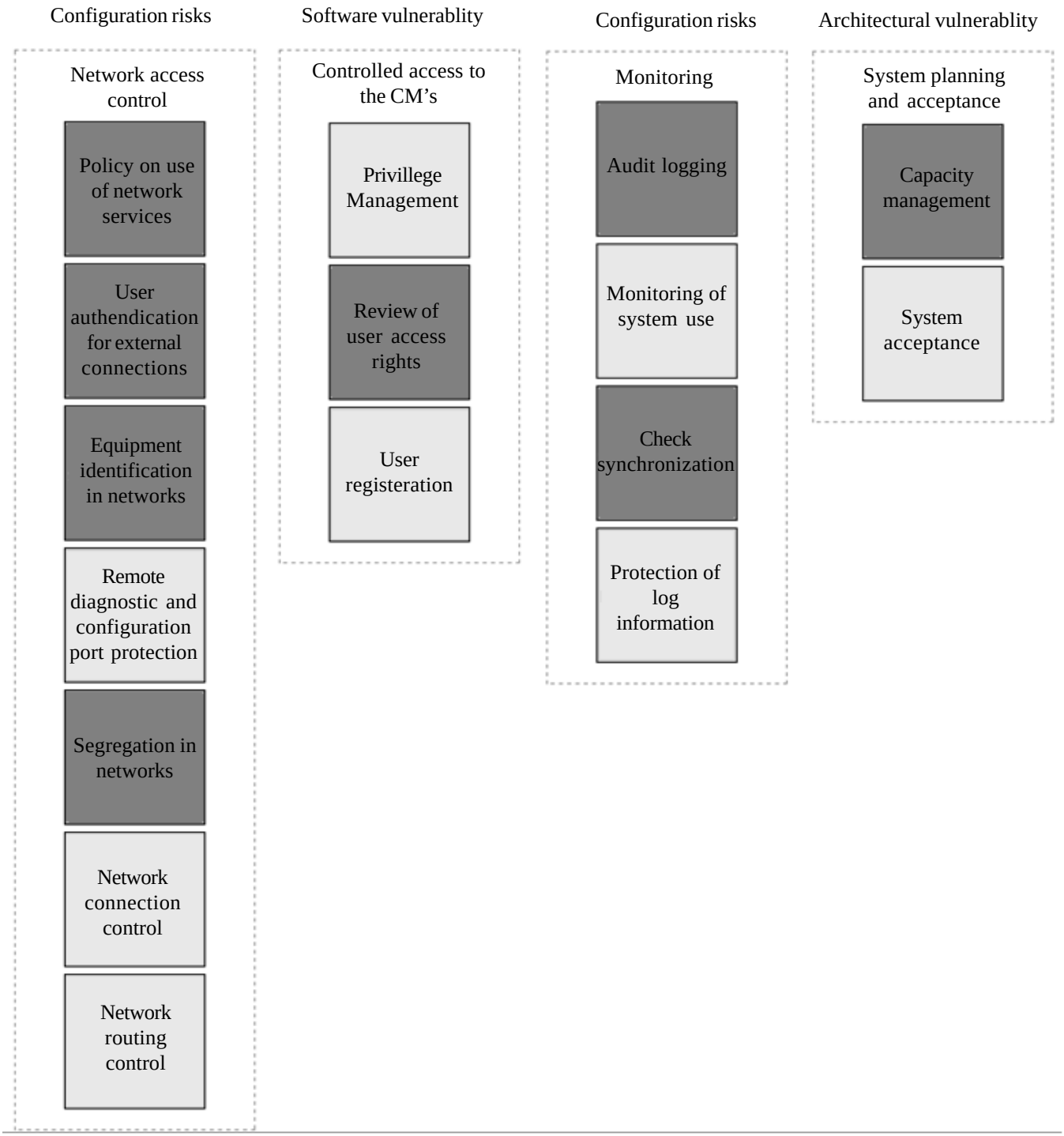

Figure 3. Example of the visualization of four areas and their corresponding subsection

$$\tilde{x} = \begin{cases} x\left(\frac{n+1}{2}\right) & \text{if } n \text{ is odd} \\ \frac{\left(\frac{xn}{2} + \frac{xn+1}{2}\right)}{2} & \text{Otherwise} \end{cases} \quad (1)$$

where the subscript is the order in the ordered set.

Because this has been done with the skewed distribution and there can be the mentioned intentional/unintentional manipulation with the degree of values and standard distortion computations cannot be used, IQR as a measure of spread will be added, which will help to define the boundaries of the admissible results. The basic IQR function [10] will divide the left and right side of the median once again to find a lower median ($l\tilde{x}$) and an upper median($u\tilde{x}$). The computation result is a set of 5 numbers:

$$\{infimum\ \tilde{lx}, \tilde{x}, \tilde{ux}, supermum\} \quad (2)$$

With this set, the data set for unusual values will be checked by searching the lower and upper boundaries, where any values in the set that will lay beyond these boundaries will be considered inadmissible.

This computation routine will take place in the summarizing of the results per tester and overall one, but the IQR will take place only in the overall computation over results and overall computation over individual criterion.

3.3 Visualization of the results

In the last step, the results are visualized. The visualization of the results is produced using a graphical notation representing the results [12] of the audit conducted by one or more owners, giving the overall rating based on the outputs of all owners.

The visualization shows the areas as components, subsections as subcomponents and the extensions as their part. These extensions are colored, meaning, that the darkest colors are the countermeasures corresponding to the biggest problems identified through questionnaire during the audit. The brightest colors, on the other hand, represent the security measures, an implementation of which is not too significantly needed.

4. Conclusion

The purpose of the presented paper is to extend existing guidelines for the auditing and assessing the virtual environment (Virtual IT infrastructure systems) and to create a methodology and a supporting tool (an expert system), which can extend existing guidelines with the utilization of a vague description, define an expert knowledgebase and therefore conduct the risk analysis (or the security audit), without the need of an expert. The guidelines are extended by the use of the knowledgebase and by the deffuzification that is transforming the vague evaluations.

At the moment, the author is in the process of finalizing the prototype in the form of a real application and the extension of the knowledgebase.

5. Acknowledgment

Presented topic is also a part of the internal grant SGS13/PrF/2013, called Fuzzy modeling tools for analysis and design of information systems, at the Department of Informatics and Computers, University of Ostrava.

References

[1] Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, 8 (6) 338– 353.

[2] Novák, V., Perfilieva, I. (1999). Evaluating linguistic expressions and functional fuzzy theories in fuzzy logic. *Computing with Words in Information*–Intelligent Systems, 2, p. 383-406.

[3] Novák, V. (1986). Fuzzy mno•iny a jejich aplikace. Prague.

[4] Klimeš, C. (2011). Model of adaptation under indeterminacy. *In*: Kybernetika, 47 (3) 355 – 368. Prague.

[5] Bartoš, J., Procházka, J., Klimeš, C., Walek, B., Pešl, M. (2010). Fuzzy reasoning model for decision making under uncertainty. *In*: 16th International Conference on Soft Computing Mendel, p. 203-209. Brno.

[6] Bartoš, J., Walek, B., Smolka, P., Procházka, J., Klimeš, C. (2011). Fuzzy modeling tools for information system testing. *In*: 17th International Conference on Soft Computing Mendel, p. 154-161. Brno.

[7] Chaudhuri, A., von Solms, S., Chaudhuri, D. Auditing Security Risks in Virtual IT Systems. *ISACA Journal*, V. 1.

[8] Bake, A. Gartner: Top Virtualization Security Risks and How to Combat Them, http://www.information-management.com/news/virtualization_security_risks-10017445-1.html

[9] Davis, D., Schiller, M., Wheeler, K. (2011). IT Auditing Using Controls to Protect Information Assets, 2nd Edition, McGraw-Hill, ISBN 0071742387.

[10] 5 Mistakes Auditing Virtual Environments (You don't Want to Make), Virtualization Under Control, WHITE PAPER, HyTrust (2011). Availible on http://www.hytrust.com/downloads/ht_wp_top5.pdf.

[11] ĊSN ISO/IEC 27001. (2006). Information technology – Security techniques – Information security management systems - Requirements. Praha : Český normalizaèní institut.

[12] Bartoš, J., Walek, B., Klimeš, C. (2012). Testing information system under uncertainty. 5th WSEAS International Conference on Visualization, *Imaging and Simulation*, p. 241 - 246. Sliema.

[13] Habiballa, H., Novák, V., Dvoøák, A., Pavliska, V. (2000). Using software package LFLC, 2nd International Conference Aplimat Bratislava, p. 355-358.

[14] Hoesing, M. (2006). Virtualization Usage, Risks and Audit Tools, *JournalOnline, ISACA Journal*, 3, www.isaca.org/jonline.