The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications
15-17 September 2011, Prague, Czech Republic

Improving the Information Security Audit Using XML Technologies

Abstract—There are described types of security threats to enterprise activity in the field of information technologies along with two ways of comparing possible costs for establishing a security system. Four main stages of auditing an enterprise information security using methods of expert examination with the XML orientation have been considered.

Keywords—audit, information security, information technologies, software, information center, expert examination, XML, XBRL, Semantic Web

I. Introduction (Heading 1)

Nowadays information is one of the most important enterprise resources. Together with the development of information technologies a risk of information leak, external interference into a functioning of information and telecommunication systems, virus infections etc. are highly increasing. For this purpose it is important to realize the protection state of valuable resources in order to resist external and internal threats to its security [1]. The search for solutions to existing problems shall be conducted not only by the enterprise itself, but with the help of external advisors, such as independent auditors. For a long time the role of audit for a business security was reduced to information security and therefore was considerably restricted [2, 4]. Under the conditions of increasing rates of business development conducting an audit of enterprise security in the field of IT becomes more and more necessary. In terms of real information security the traditional audit does not meet enterprise needs, since it is usually limited to independent expertise of financial reports and other information about financial and economic activities of the enterprise. Thus there is a need to introduce audit into new spheres, including IT, that may improve the system of enterprise information security. This is particularly relevant for post-soviet countries, such as Ukraine, where audit of enterprise information security is in a rudimentary state [7].

It should be mentioned that solving a problem of strengthening an enterprise security in the field of IT by means of audit is complicated by the fact that it is handled by specialists in several spheres of knowledge simultaneously and requires appropriate competence of the researchers. That is why our goal was to develop scientifically grounded recommendations on conducting an audit in this field based upon researches, as described below.

II. Approach to Conducting an Enterprise Audit in the Field of Information Technologies

One can assume that the process of auditing an enterprise information security in general is similar to classical audit, which means that it should contain 4 main stages. (i) planning and preparation, (ii) setting goals (tasks), (iii) conducting audit, (iv) final report presentation.

Authors conducted an analysis at the stage of *audit preparation* that allowed to outline the following types of security threats to enterprise activity in the field of IT:

- Lack of regulated access to data files and software using
- Lack or incompleteness of information security support system
- Lack or incompleteness of the integral system for the assessment of security threats [3-6]

Besides, it is necessary at the *preparation stage* to compare possible costs for providing security with perceived benefits of security system establishment. It can be reached in two ways:

- assessment of cost savings that are achieved as a result of security measures;
- calculation of return on investment (ROI) that includes evaluating actual (net) cost of resources under protection [1].

Proper calculation of costs for strengthening enterprise security should be based on usage of the following indicator system:

- Total cost for implementing the measure
- The amount of damage averted
- The amount of damage caused
- Efficiency of the measures implemented as a result of dividing the difference of damages adverted and caused by the total cost.

Undoubtedly, the security system of every enterprise should be absolutely individual. Its completeness and effectiveness depend on the following: existing legislative framework; scope of material, technical, and financial resources provided; quality of software and data storage; completeness and correctness of functional chart for employees of corresponding divisions etc.

Concerning *goals (tasks)* of the audit at the *(ii) stage* authors offer to concentrate, firstly, on job descriptions and personal responsibility of executives (information center employees), including their professional training in context of information security and secondly, on verification of the procedure for making changes, presence of appropriate instructions and regulations concerning data security providing in the Information Center. We should emphasis – as a prime importance –on implementation of the flexible and sufficiently complete indicator system for the security assessment including the financial measure of damages and losses (see above) in a case the information security system was failed. Extension of audit possibilities and improvement of the information security should be reached because of using the XML and XBRL standards and universal means for representation of information security indicators and implementation of security international standards in future.

At the stage of *conducting* an audit a state of reaching above mentioned goals is assessed. This means that methods and means of Information Center data security shall be examined along with the qualification level of appropriate employees by means of interviewing them. Moreover, the auditor should verify the following: correctness and efficiency of computer hardware in the Information Center; guidelines and procedures for collecting, storing, and duplicating data; inventory and functionality of operating systems; job descriptions of Information Center employees; provision of Information Center with appropriate security measures in order to eliminate unauthorized access to it; and presence of measures for control and monitoring of internal and external environment in order to provide protection against disasters. Separating the unit of the information security by XML and XBRL means including financial measure will allow to work through time the indicators and mechanisms of information security audit in limits of the proposed “extensible language of information security audit(eXtensible Security Audit Languauge, or XSAL), and facilitate putting into operation of information security global standards. In such context the tool setup of information security audit requires to introduce appropriate means oriented on Semantic Web platform. One of such projects is a semantic platform Word Press within a joint project of the Research Center of Tax Problems, National University of State Tax Service and Research Institute for Intelligent Computer Systems, Ternopil National Economic University, Ukraine aimed for creating the virtual tax office for the service support in the area of e-tax accounting [8].

In view of the deficit of diverse professionals authors support conducting an audit of enterprise information security in an expert way. The purpose of conducting an expert examination is to assess the state of Information Center and enterprise information security as a whole and develop recommendations on protection of information resources against threats. Expert approach is based on risk analysis, on the ground of which an auditor determines an individual set of security requirements for the information system in question. The said set of requirements should mainly consider: (i) peculiarities of the given information system, (ii) its functional environment, and (iii) security threats that exist in it. In addition, the expert detects other deficiencies in information security system based on his/her personal experience. In general, expert examination provides possibility to prepare reasonable proposals for protection of the enterprise in the field of IT.

As a result of an audit there are formed recommendations concerning strengthening enterprise security in the field of applying IT, for instance, verification of appropriate software and its modification (if necessary), taking measures to keep data privacy and protect software etc. The results of enterprise security audit in the field of information technologies should be summarized in the final report (package of final documents) according to the format and standards XML, XBRL, as well as XSAL one proposed by authors.

III. CONCLUSIONS

Based on the analysis conducted at the stage of preparing an audit authors created a list of threat types to the security of enterprise activity in the field of information technologies and offered two ways to compare possible costs for establishing a security system.

There were determined and developed recommendations for conducting audit of enterprise information security by using methods of expert assessment that has academic and practical value both for Ukraine and other former Soviet countries.

Authors proposed a mechanism of information security audit within XML concept that allows forming the basis of further taxonomies and knowledge’s bases for the secure IT.

REFERENCES:

[1] V.P. Borodiuk, A.V. Lvova. Strengthening the economic efficiency of information security system. Bulletin of Moscow Energy Instittute. – 2007. – no. 4. – p. 139-142.(In Russian)

[2] V.I. Podolskii, N.S. Shcherbakova, V.L. Komissarova. Computer Audit. – Moscow: Yuniti-Dana, 2004. – 128 p. (In Russian)

[3] N.V Grishina. Organization of complex information security system./ N.V Grishina – Moscow: Gelios ARV. – 2007. – 256 p. (In Russian)

[4] V.O. Golubiev and etc. Information security: issues of combating crimes in the area of applying computer technologies. Humanities university “Zaporizhzhia Institute of State and Municipal Governance”. – Zaporizhzhia: Prosvita. – 2001. – p. 236-246. (In Ukrainian)

[5] Porter B., Hatherly D., Simon Jon. Principles of External Auditing. 3rd edition. – Wiley, 2008. – 816 p.

[6] Smieliauskas W., Bewley K. Auditing: An International Approach. – McGraw-Hill Ryerson Higher Education. 2006. – 800 p.

[7] Audit of Intranet Security – S.A. Petrenko, 2002. (In Russian)

[8] Melnyk P. V., Rippa S. P. and etc. E-Tax Service: Essence and Perspecives of Implementation.-Irpin’:NUDPSU,2010.-332p.(In Ukrainian)