ISSN No. 0976-5697

Volume 7, No. 6(Special Issue), November 2016

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Various Issues in Expert System for Information Management and Audit

Gurinder Kaur
Assistant Professor
Guru Nanak College, Budhlada

Pooja Rani
Assistant Professor
Guru Nanak College, Budhlada

Shabeena Garg
Assistant Professor
Guru Nanak College, Budhlada

Abstract—Today's organization are more concerned towards the security of information. This can be achieved with the help auditing technique. Due to complex process, we move to expert system for auditing. In this paper we will discuss expert systems for information security management and auditing and various implement issues in expert system.

***Keywords*—audit, information, security, expert system**

I. INTRODUCTION

Today organizations are facing with a wide range of potential threats to their information security (IS). One of the best ways to estimate, achieve and maintain security of information is an Information Security auditing. Auditing is a complex and many-steps process involving high-qualified experts in IS, what makes it a quite expensive process. There are many types of audit, including certain security standards (e.g. ISO 27K) compliance audits. Generally, information security audit is conducted in the following steps[1]:

1. **Scoping and pre-audit survey:** finding the main area of focus; establishing audit objectives.
2. **Planning and preparation:** usually made an audit plan/checklist.
3. **Fieldwork:** gathering evidence by interviewing staff and managers, reviewing documents, printouts and data, observing processes in action, etc.
4. **Analysis**: sorting out, reviewing and analyzing of the accumulated evidence in relation to the objectives.
5. **Reporting:** reviewing all previous stages, finding relations in the collected information and composing a written report.
6. **Closure**.

Each of the stages is included with a large amount of information, which needs to be recorded, organized and, finally, analyzed. One of the step taken in reducing expenses and conducting audit is using of helping tools for identifying the gaps that exist between certain security standard and an organization's security control, like checklists and questionnaires. For example, ISO 17799 [2] Checklist gives number of audit questions (like "Whether responsibilities for the protection of individual assets and for carrying out specific security processes were clearly defined."). ISO IEC 27002 2005 (17799) [3] Information Security Audit Tool offers several hundred audit questions, stated in yes-no form (e.g. "Have you reduced the risk of theft, fraud, or misuse of facilities by making sure that all employees understand their responsibilities before you hire them?"), pointing to security practices that need to be implemented and actions that should be taken (in case of "no" answer to question). So, the auditing may be viewed as a process of asking questions and reviewing answers to produce recommendations.

Of course, these tools are very useful to auditors and security related staff. But the questionnaires don't give an overall impression of organization IS level, entries of the checklists are too general (not concrete, not related to particular organization's actual policies, procedures, etc.). Such kind of disadvantages doesn't allow them to be used independently, without any additional security measurements.

Another good tool for the audit is to develop a knowledge base that will provide information for Chief Information Security Officers (CISOs) [4] and will help them to find the right decisions on the information security policy. Key components of the knowledge base are: "Asset", "Source" (standard), "Vulnerability," "Step" (a refinement of the part of "Guideline" in a special section of the standard) and others. Every "Step" is linked with an asset it protects, type of vulnerability it is against and also cross-references to other stored guidelines. The proposed tool provides a search in the knowledge base for guidelines in standards using their components. As a result, some meta-model of the security standard recommendations could be constructed. As of highly expensive process of information security Auditing in terms of high cost of different resources (time, people, expenses) the reducing the cost of the audit process is a priority for any organization. Automating the audit process by making intelligent software (expert system) can significantly reduce costs, since the main work on decision-making is done automatically, based on computer analysis of the situation and giving guidelines and recommendations. We think that expert systems have much to offer in the case of IS audit automation. Expert systems (ES)

978-93-85670-72-5 © 2016 (RTCSIT)

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India

approach firstly fits question-answer format of auditing, secondly, ES function on the basis of meta-model that reflects knowledge in this field. Expert in particular field thinks and implementing common human logic can give a system that is able to assess the situation and make decisions. An Expert System in Security Audit, designed for automating some audit procedures, like identifying potential security violations by analyzing system logs. But the application of the methodology of expert systems in IS auditing in the broadest sense remains largely untouched. Our task is to study and solve the problems of development of expert systems in a wide range of information security audit, which includes aspects of computer security.

II. EXPERT SYSTEM IN IS AUDIT

An expert system (ES) is a computer system that helps in the decision-making ability of a human expert. The knowledge in expert systems, commonly represented in form of IF-THEN type-rules, may be either expertise or knowledge that is generally available from written sources. We think that in IS field, along with human knowledge, security standards' (ISO/IEC, COBIT and ITIL, in particular) recommendations can also serve as a source of expertise and may be translated into rules. Some of advantages of the use of expert systems, particularly in IS field are [5]:

• **Reduced cost**- Development of an expert system is relatively inexpensive. Taking into consideration an opportunity of repeated use by multiple organizations, the cost of the service per client is greatly lowered.

• **Increased availability**- Expert knowledge becomes available using any suitable device at any time of the day. Web-based expert systems open up ability to access expertise from any Internet connected device.

• **Multiple expertise**- Using knowledge from multiple sources increases total level of expertise of the system. In case of IS, a combination of number of security standards' recommendations and knowledge of several independent specialists could be used.

• **Time saving**- IS auditing is a time consuming process. Expert systems at some phases of audit (analysis of gathered evidence, reporting) can save days (or weeks) by faster responding (in comparison with a human expert) and reducing amount of paper work.

• **Steady, unemotional, and complete response at all times**- By the use of programs, human factor influence decreases.

Expert system is developed as a platform which keeps the knowledge base and automated gathers information of the object, analyzes using fuzzy logic and makes conditions based on the results. System is used for information security audit. The main task of the expert system is to completely replace the preaudit, which usually takes a very long time. Using an expert system, we not only save time, but also eliminate the possibility of errors in the calculation of results. The architectural scheme of the application is pretty simple; it does not have complex links. The user interface is designed for auditors or employees of the company, who provide IS audit. Through the interface an auditor gives to an application requested data: information about the requirements of information security made in the protection of information. "Figure 1" shows the overall picture of the considered expert system, which consists of five parts: Database, interface for experts, interface for risk managers, interface for analytics and interface for information security officers. At first, we will get started with the description of Database. It contains questions, the list of users, answers, question weights, risk levels, recommendations, analysis results and tools. It is a main component of the Expert system, as each other component directly interacts with it. Top of the figure 1 is an interface for the target company. Employees are divided into categories. Interface for Information security experts/professional is shown on second part. Experts pass authorization phase, after that they determine the ranges for questions as set of linguistic variables like LOW, MEDIUM and HIGH that is relevant to set of numeric values. Third part presents an interface for risk managers. It is the same as for experts: the authorization and evaluation of risk level for questions. Fourth part shows the interface for analytics: authorization and own interface, in which analytics can run different calculations of results and take output results. Interface for providing recommendations based on the outputs by the Information Security Officer is shown in sixth part.

III. ISSUES OF EXPERT SYSTEM

We are facing a no. of issues in expert system of audit. In this paper we will discuss design and implementation issue in expert system.

A. Design Issue

Main issues while designing an expert system are:-

- While designing an expert system, we have to decide the agent that should included as several agent helps in designing an expert system. [7].
- Portability, stability, resilience, and security of the agents and system
- We have to design performance behavior according to the environment.[8]
- We have to identify type of feedback from learning.
- We should consider representation of data before designing expert system
- Availability of prior knowledge
- System should cost effective. [9]

978-93-85670-72-5 © 201

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India

B. Implementation Issues

Some of the implementation issues are:-

- During implementation, firstly we have to make questionnaire page.
- Questions should be related to security and standards which should assigned value between LOW, MEDIUM and HIGH.
- Risk managers should have good viewpoint of security.
- Questionnaire should contain the concept of Threat i.e. unwanted incident that can lead to loss of organization.[10]
- Answers of users should convert into weights for analyzing purpose.
- Analyze the risk level based on weight.
- Based on risk level, expert system should give recommendation.[6]

IV. CONCLUSION

This work was done to study various design and implementation issues in providing efficient information security management procedures. It has described the development of an expert system for these purposes. Importantly, expert systems will be based on the concept of intelligent information technologies capable of considering problem situations from various perspectives in their further development. A variety of software products designed primarily to help the decision making person make a choice of solutions in accordance with the requirements and needs of the organization.To conclude, we can say that this is just a technique for ease decision-making processes may bring significant practical value in information security audit and fuzzy expert systems development.

REFERENCES

[1] Hinson, G. 2008. Frequently Avoided Questions about IT Auditing - http://www.isect.com/html/ca_faq.html

[2] Val Thiagarajan, B.E. 2002. BS 7799 Audit Checklist. - www.sans.org/score/checklists/ISO_17799_checklist.pdf

[3] ISO IEC 27002 2005 Information Security Audit Tool - http://www.praxiom.com/iso-17799-audit.htm

[4] Stepanova, D., Parkin, S. and Moorsel, A. 2009. A knowledge Base For Justified Information Security Decision-Making. In 4th International Conference on Software and Data Technologies (ICSOFT 2009), 326–311.

[5] Giarratano, J., and Riley, G. eds. 2002. Expert Systems: Principles and Programming. Reading, Mass.: PWS Publishing Company.

[6] Kanatov, Atymtayeva and Ygaliyeve, 2014. Expert systems for Information Security Management and Audit. Implementation phase issues.In SCIS&ISIS.

[7] Russell, S. & Norvig, P. (2003). Artificial intelligence a modern approach (2nd ed.). Upper Saddle River, New Jersey: Prentice Hall.

[8] Mariana, 2007. Intelligent System for Information Security Management: Architecture and Design Issues. In Issues in Informing Science and Information Technology Volume 4, 29-43.

[9] Wallich, P. 2003. Getting the message. IEEE Spectrum, 40 (4), 39-42.

[10] Muromtsev D. 2005. Introduction to expert systems. St. Petersburg.: St. Petersburg State University ITMO, 93 p.

978-93-85670-72-5 © 201

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India