Main Issues of the Software Development for Knowledge Base Processing in the Intelligent Applications for Information Security Audit

LYAZZAT ATYMTAYEVA, ASSEL AKZHALOVA, KANAT KOZHAHMET
Computer Engineering Department
Kazakh-British Technical University
Almaty, Tole bi str., 59
KAZAKHSTAN
l.atymtayeva@gmail.com, assel.akzhalova@gmail.com, kanik85@gmail.com

Abstract: - This paper describes the main stages and features of the software development for intelligent systems in information security audit based on international safety standards ISO 2700x. We present the description of the main processes of auditing information security, ontology and questionnaires development methodology to determine the level of information security, safety assessment methods based on specially designed components and metrics.

Key-Words: - Expert Systems, Information Security Audit (ISA), Information Security Management System (ISMS), Fuzzy sets and Logic

1 Introduction
The main purpose of the audit of information security based on standard ISO 2700K is determination how well, correctly and promptly delivered an Information Security Management System (ISMS) in a company or organization. By providing the analysis of standards ISO 2700K, we can highlight the following main features of standards 2700K.
The standard 27001 can serve as a basic domain for all standards where can be shown the main requirements of Information Security Management System (ISMS) and itemized criteria for any company [1]-[3]. ISO 27002-27005 standards are complementary facilities which show the basic methodology, techniques and controls for using as a support and guide by auditors on information security (IS). Thus, it is enough to use only the individual chapters of ISO 27001 for providing good IS analysis.
In the process of information security audit we can identify a number of basic steps. The main stages of information security audit we can show as following:
I Goals definition
- to understand the purposes and benefits of the implementation of the ISMS
- to get management support for the implementation and commissioning of the ISMS
- to distribute responsibilities according to ISMS
II Organizational issues
- to create a group for ISMS implementation and support
- to train a group for ISMS implementation and support
- to define the scope of ISMS
III Initial ISMS analysis
- to conduct analysis of existing ISMS
- to determine the list of works to finalize the existing ISMS
IV Defining ISMS policy and objectives
- Define an ISMS policy
- Identify objectives for each process of ISMS
V Comparison the current situation in the company regarding ISMS versus international standards requirements
- to conduct training for ISMS responsible persons to get main knowledge of ISMS standard requirements
- to scrutinize the requirements of the standard
- to compare the existing conditions of ISMS in company versus the standard requirements
VI Planning of the ISMS implementation
- to define the list of measures to achieve the requirements of the standard
- to develop guidelines for information security
VII Establishment of Risk Management System
- to develop the procedures for the identification of Risks
- to identify and rank Assets
- to develop catalogue for "Modules"
- to identify responsible persons for Assets
- to estimate the Assets
- to identify threats and vulnerabilities for assets
- to develop catalogue for "Threats"
- to calculate and rank Risks
- to develop a plan to reduce and mitigate the Risks
- to develop catalogue for "Countermeasures"
- to identify guideline for non-applicable security controls
- to develop guideline for the applicability of security controls

VIII Development of ISMS documentation
- to define the list of documents (procedures, records, instructions)
- to develop procedures and other documents including
  - Administrative procedures
  - Technical procedures
  - Records management
  - Technical notes
  - Instructions
- development and implementation of ISMS documents

IX Personnel training
- Training the heads of IS responsible departments to the main issues of Information Security requirements
- Training of all personnel to the main requirements of IS

X Development and adoption of measures to ensure appropriate work of ISMS
- Implementation of administrative, academic, and technical remedies

XI Internal ISMS audit
- Selection of internal ISMS audit team
- Planning internal ISMS audit
- Conduct internal ISMS audit

XII ISMS analysis by senior management
- Analysis of the ISMS by senior management

XIII The official launch of the ISMS
- The order of the Implementation of ISMS

XIV Notification of stakeholders
- Informing customers, partners, media about the launch of ISMS processes in company

In this consideration of the main stages we can assume that the expert system carries the role of the auxiliary tool for the arrangement the process of the audit of the information security according to the main stages of ISMS. In order to comply this audit process with information security standards we should use topology table of ISO 27001 and 27002. In the intelligent system for information security audit we consider the main points of released standard ISO 27001:2013, in which there are some differences from the current standard ISO 27001:2005. Mainly changes were made in Chapters 4, 5, and 6, as well as in chapters 3, 11, and 12 [11].

Due to intrinsic uncertainty in safety and security decision making, it is very difficult to apply quantitative approach to the security measurement in many critical managerial tasks. For this reason, they are usually handled by a significant number of human experts. On the other hand, this causes unnecessary inconsistencies, together with tis high expenses and long duration. Consequently, we expect a significant demand on a framework for handling such uncertainties such as fuzzy logic.

Fuzzy logic may be viewed as an attempt at formalization and mechanization of two remarkable human capabilities: (1) to reason and make rational decisions in an environment with imperfect information and (2) to perform a wide variety of intelligent tasks without precise measurements or intensive computation [6]. Experts in information...
security may almost always utilize both of the capabilities in their work.

There are plenty of applications of fuzzy logic in risk management and decision making for matters related to security and safety [6-11]. Various application aspects of fuzzy logic in system failure engineering are discussed in reference[8], which include a fuzzy logic application in fault diagnosis, in structural reliability, software reliability, human reliability, safety engineering, security engineering, risk engineering, and quality control. A simple fuzzy expert system for risk calculation based on likelihood of the event and severity of its consequences is proposed in reference [9]. Development of Security Risk Factor Table (SRFT) is described in reference [7], which consists of several factors affecting security such as location and visibility of refinery plant and range of their values such as high and low visibility of rural and urban location. In addition, security score evaluation on the basis of single or multiple experts using linguistic terms is calculated. In reference [10], a similar method is utilized to evaluate network security systems by different vendors. A new technique based on fuzzy logic is developed for prioritizing failures for corrective actions by assessing risks of the failure based on severity, frequency of occurrence, and detect ability [6]. Trivially, fuzzy logic and its related approach resolve critical issues in traditional methods of risk evaluation based strictly on numerical methods such that:

1) it allows the analyst to evaluate the risk associated with failure modes directly using the linguistic terms that are natural for human experts in making the criticality assessment;

2) ambiguous, qualitative, and imprecise information, together with quantitative data, can be used in the assessment and they are handled in an integrative and consistent manner; and

3) it gives a more flexible structure for combining the severity, occurrence, and detectability parameters.

In short, approaches based on fuzzy logic allow utilization of generalized, i.e. imprecise or incomplete information, whereas traditional numerical methods may only work well with precise numbers. Moreover, fuzzy logic based approaches are much more compatible with human reasoning, as quantities can be represented naturally in linguistic terms. This means that the inputs, as well as the outputs, to such systems can be partially or entirely linguistic so that human experts may likely interpret those naturally. When necessary, consistent numerical representation can be generated as a result of defuzzification.

As can be seen, fuzzy logic was applied effectively but only in particular stages of security assessment, more precisely, in its risk assessment. Actually, security risk management requires a systematic approach to analyze various security risks in a comprehensive manner [11]. Its analysis is usually performed qualitatively using the best judgment of the experts and involves the following steps:

Asset characterization: Identifying assets to be secured and their value to an organization.

Threat assessment: Identify and characterize threats against assets and evaluate their potential to happen.

Vulnerability assessment: Identify potential security vulnerabilities that could be exploited by threats.

Assessment of security risks: Calculate the risk on the basis of a likelihood of an event and its consequences.

Recommendations: Identify and evaluate risk mitigation options.

You can find fuzzy variables and terms in every step, e.g., asset value, threat likelihood, vulnerability severity, security risk, effectiveness of a risk mitigation measure. Therefore, we believe that the use of fuzzy logic needs to be broadened to all stages of the security assessment. Apart from that, we need an approach to acquire and apply various kind of knowledge about information security management, including concepts, facts tips, and experiences within it. We believe that expert systems and their development methods highly likely suits the best here.

At present, the means and tools of information security audit include such international standards as ISO27002, ITIL V3 and COBIT 4.1. Existing international standards for information security can unify the requirements that likely serve as the basis for creating the expert systems. The advantage of such expert systems is lies under the conjunctive use of various knowledge as behavioral models of the experts, and the storage of data begin used or generated by procedures of (fuzzy) reasoning and decision-making.

A whole or partial automation of the security audit process should take place through the deployment of such expert systems using fuzzy logic. This should offer significant advantages for its costs, workload and duration. The presented work suggests a way to develop fuzzy expert systems in information security audit, specifically at
the first stage of its development, i.e. ontology and knowledge base building.

2 Methodology of ontology and questions design in expert system for ISA

We have developed an expert system that is based on the data collection and analysis obtained during the survey of staff of the auditing company [12]-[15]. Data collection is being held by interviews and observations which are realized as a dynamic module dependent on a few criteria. The survey is based on the set of issues defined by the company employees. Data collection is carried out by experts by means of questionnaires or oral interviews asked from certain officials of the company. These interviews are recorded, logged and analyzed by an expert that conducts the survey.

The main criterion for the development of questions is an approach audit compliance with ISO Standard 27002. The questions are set up by this format in order to ensure that responses give a general picture of conditions to maintain information security in the company. Another approach is to use best practices that taken into account the experience and expertise of the auditor. It should be noticed that it needs to take into account that the question asked during the audit is intended for several staff members and it can be set at one time for all members.

The module of questions in the expert system has the following structure: the question, the answers, the weighting factors responses in the form of a fuzzy data.

All questions set up in the expert system use fuzzy logic approach, therefore, during their formation it should be taken into account that the answers will be not only in the format yes/no. Those questions, in terms of fuzzy logic, are the nature of the correction and provide an opportunity to determine a degree (percentage) of compliance to the standard. For example, weak control of the physical security such as control of physical inputs (see ISO/IEC Standard 27002, 9.1.2, "Control physical inputs") depends on correct use of the authentication control and appropriate monitoring which is subject of the turnover of staff at the professional security guards and verification of their compliance. This deficiency may cause physical damage to assets, theft of important information, etc. Due to the fact that it is impossible to assess the possibility of the adverse situation it is necessary to use fuzzy terms for the data submission and to take into account of the impact of possible factors and rules [16]-[20].

In accordance with ISO Standard 27002 "Control operational software" let us look at the "step" in the section 12.4.1 - "update operational software, applications and software libraries should only be performed by qualified administrator with the appropriate level of the permission (authorization)". In this case, it is necessary directly determine if there is sufficient staff trained then whether he/she has qualified knowledge and skills. The administrator qualifications depends on his/her experience and knowledge. For the system simulation an experience can be defined as a numeric value.

It is more difficult situation in case with knowledge modeling. Naturally, human knowledge even in a limited area could not be assessed by one question. In this case, it is necessary to use not only direct questions but also indirect ones defining skills of an administrator. In some test questions it can be provided specific parts (to form the special question), for example [20]:

1. If you are installing NTFS permissions for individual network drives which of the following options should be allowed to the user as default settings?
   Answers: Full access / change / Read and Execute / read / write.

2. What characters always end in the common names of administrative folders?
   Answers: 

3. Which is equal to 1 kilobytes (KB)?
   Answers: 512 bytes / 1000 bytes / 1024 bytes / 1028 bytes / 2048 bytes and so on.

Each of the questions and answers has its weight (in %) and it is defined by fuzzy variable (included in the range of values).

2.1 Determining Roles in the expert system

Another important aspect of auditing information security is to define roles and the degree of the liability of employees in the company. At the preparation stage of the company for auditing of information security one of the important facts is the definition of competence of any employees of the company as well as the appointment of a chief moderator responsible for auditing information security. Summarizing above it may be noted the fact that the questions which will be set by a certain competent person of the company will have different coefficients of significance. The roles in the expert system we take into account an approach
of best practices in the face of experts on information security audit. Information security experts define multiple roles and types of users in an expert system, namely: ISMS Manager, management correction, ICT managers, staff, Business Managers / Info owners, IT staff, partnered (staff), and end users. The following shows the description these categories.

- ISMS Manager is/are responsible person/persons in the organization of the information security audit
- Management correction - managers and the main leaders in the organization
- ICT managers - Managers of IT departments and their correspondent departments
- IT staff - IT staff of the company
- Business Managers / Info owners - CEO Leaders
- IT staff, individual (staff) are the heads of the other units in the organization
- End Users are the end-users and the staff of the organization.

This type of separation onto the category is defined by the standard division of responsibilities and conforms according to ISO 27001:2013. During the process of information security audit (ISA) it has to be taken into account the fact that each of above categories in this company has varying degrees of responsibility and competence of ISA. Based on the above it should be identified the coefficient of responsible employees and liability categories. Since the interviewing a company it should be identified the questions and their degree of influence on a certain point in the standard ISO 27001:2013. It should be noted the feasibility of using vague terms "degree of influence" of question which also points to the importance of the use of fuzzy set theory and logic in the construction process as well as an ontology for information security audit process according to ISO 2700x.

2.2 Design issues in the development of expert system

The development of an ontology, in accordance with ISO 2700x:2013, we need to take into account the fact that in determining of any questions to any parties it is necessary to allocate consolidation ratios that often exceed their relevance to all the dependent points of ISO standard. Thus, the questions have become correlated in determining of the influence evaluation.

Each sub-item in ISO 2700x:2013 determines the group of questions which, in turn, had a different influence degree to the specific point cumulatively representing a full meaningful consolidation ratio (quantified as 10). In other words, the questions in any subparagraph depending on their number must be in the amount of consolidation ratios that is in total 10. For example, if we have two questions, they may have a weight (5 and 5) or (2 and 8) and so on. An example of the questions is shown in Figure 1.

![Fig.1 Presentation of questions in the ontology of the expert system and their degree of influence](image-url)
The tree of ISO 27001:2013 standard consists of 3 branches [17]. The one of the major problems in auditing information security by ISO 27001:2013 is a different perception of sub-items in the standards and their relevance to their own predecessor. For example, the main item 6 Planning of the standard has two sub-items where each of them has its own weight but, in general, they should not affect the overall result. The same graduation there is in each subparagraph of the standard.

The implementation of such approach can qualitatively show an overall assessment and periodically give different results and it is very important in an expert system where the design is based on the fuzzy logic.

Figure 2 shows the model compliance of items of the standard and the ontology of Expert System (ES).

Some of the questions in the system have a link according to the "root-child" principle that affect the nature of the detailed survey. This link should not be appear, however, in some situations it must be reinvented.

The proposed system also provides for coefficients of responses affecting to the generation of recommendations [21]-[34].

We have developed a Web-based interface (on local language) for data entry to the expert system where questions are in several types: multiple choice, text field, a numeric field, and true/false (Figure 3).

### 2.3 Knowledge Base in expert system

At the moment, for the expert system based on ontology, we have developed rules using FRIL programming language. The rules in the system are organized in a format: IF (group of statements) THEN some_value is (low/moderate/good/high).

Based on the developed tables for the building of rules, the diagram is designed to organize the rules. The view of the rules in the language FRIL can be submitted in the form of the following form:

**IF user has full access to the Internet (can open and download files, etc.) AND virus protection on user’s machine is not properly configured AND user has an access to some confidential information THEN there is a possibility of information theft.**

**IF user has full access to the Internet AND virus protection on user’s machine is not properly configured AND user has an access to confidential information AND confidential information is available when logging in from the outside (not from local network) THEN there is a BIG possibility of information theft.**

**IF QuestionID501Answer2 is VERY LOW THEN 2Control411 is LOW**

**IF QuestionID501Answer2 is LOW THEN 2Control411 is MODERATE**

**IF QuestionID501Answer2 is MODERATE THEN 2Control411 is GOOD**

**IF QuestionID501Answer2 is GOOD THEN 2Control411 is GOOD**

**IF QuestionID501Answer3 is VERY LOW THEN 3Control411 is LOW**
IF QuestionID501Answer3 is LOW THEN 3Control411 is MODERATE
IF QuestionID501Answer3 is MODERATE THEN 3Control411 is GOOD
IF QuestionID501Answer3 is GOOD THEN 3Control411 is GOOD

IF QuestionID501Answer4 is VERY LOW THEN 4Control411 is LOW
IF QuestionID501Answer4 is LOW THEN 4Control411 is MODERATE
IF QuestionID501Answer4 is MODERATE THEN 4Control411 is MODERATE
IF QuestionID501Answer4 is GOOD THEN 4Control411 is GOOD

IF QuestionID501Answer5 is VERY LOW THEN 5Control411 is MODERATE
IF QuestionID501Answer5 is LOW THEN 5Control411 is MODERATE
IF QuestionID501Answer5 is MODERATE THEN 5Control411 is GOOD
IF QuestionID501Answer5 is GOOD THEN 5Control411 is GOOD

### 2.3.1 Methodology of the rules development in the knowledge base

Based on expert assessments, vision and knowledge of the best practice, it can be argued that the main criterion for determining the model of compliance results of data output after analysis in expert system it is necessary to determine answers to all the questions in the audit process. It should be noted four major characteristics for the formation of rules in the ontology of knowledge base, namely [35]-[37]:

1. Structural definition of the rules: Rules and regulations are being developed in the knowledge base in an expert system must have a structural view.
2. Optimization rules: Rules may be amenable to optimization
3. The integrity of the data: Data must have a regular template
4. Logging data: Data in the system must be permanently saved

We have a common model of the audit process which is based on the following procedures:

1. Data collection
   a. The definition and the appointment of users in the system
   b. The definition of assets in the company (to determine the risks but not to conduct an audit on the model of conformity)
2. The beginning of the audit
   a. Testing of all staff system
3. An analysis of the data in an expert system
4. The results
   a. An overall situation
   b. Recommendations generation

### 2.3.2 The definition and the appointment of users in the system

Information security audit process includes the definition and assigning users in the system. In this expert system, it is necessary to define the user categories which are represented by users of auditee companies. Based on data received from the experts as well as information security and ontology, in the expert system we defined six categories of users: ISMS Manager, Manager correction, ICT Manager, IT staff, business managers, other business managers, and...
individuals/staff which have different degrees of responsibility in the System Management of Information security of auditing company. We provide the list of categories users which should be defined in the system on the stage of initialization information security audit:
- ISMS Manager, the main person or group of persons responsible for auditing of the company that have a very high degree of responsibility in the audit as well as they should comply to the ISMS Manager competence model.
- Manager Representative - The head of the business/organization. The main person who is an initiator of the audit and usually the head of structural division of the company.
- ICT Manager is the Information security manager of the company. In the case if the responsible company has a department or division for information security all members of this division are ICT Managers.
- IT staff are the staff of the IT Division/Department of the organization or its affiliated group of people in the company responsible for the IT infrastructure of the company, and in certain cases, it may be the affiliated company.
- Business Managers are the ordinary managers in the auditing company that have relationship with ISMS.
- Individuals/Staff are all the rest of the staff of the auditing company.

In the expert system the degree of responsibility is defined by above mentioned division of powers in the process of ISMS. Based on the ontology of the information security, different categories of persons (the above-mentioned five categories) have various degrees of responsibility for the organization and different levels of ISMS. Expert system asks different types of questions or those same questions but metrics of the responses have different values of coefficients.

2.3.3 The definition of assets in the company (for determining the risks but not for conducting an audit of the model of conformity)
The main stages in Auditing Information Security process include the identification of assets of the company. Entering the data assets of the company is usually implemented by the head of ISMS. The system has special interface for input data where by selecting specific characteristics of company performance the system can receive an overall picture of the company's assets.

2.3.4 Testing of all staff by expert system
The most basic step in the process is the Information Security audit is survey of all employees of the company where all responsible persons in the company should reply to a number of questions asked by the expert system. As the system has an access through a web-oriented environment users will have logins and can test and respond to the questions in a personal cabinet.
Next step, after the interview the system starts data analysis.

2.3.5 An analysis of the data in an expert system
An analysis of data in the expert system is done by the software complex support logic programming. The main interpretation of rules is a programming language FRIL. All input data obtained by the system work according to the schema "sequence". In other words, first, all of the data should be entered into the system and further they interpreted in format convenient for FRIL. After receiving data the module of the expert system processes data and sends them again to the web server of the expert system.
The main objectives of the analysis are:
- Building of the complete list of the most dangerous vulnerabilities and threats [35]-[37].
- Design an overall model of the potential attacker
- Assessment of the degree of severity threats information security and the possibility of their use of a potential attacker to the implementation of the unauthorized action
- Development of recommendations and their implementation allow to minimize the threats.

2.3.6 An overall situation
The result of the data analysis is a web-based dynamic report which will reflect the main points of the audit information security. In this report all ISMS vulnerability is shown. As a result, the report shows all answers of all categories of staff [37].

2.3.7 Generation of the recommendations
At this stage the main recommendations for the auditing company will be determined by the all criteria of ISMS. All data in the system are displayed in info graphics in which it can be viewed the reports on all the details and points.
As well as using the ontology of the expert system for auditing information security we have developed and implemented the technical specification of the expert system.
3 Conclusion
As a result of the activities involved in the implementation it was studied the main problems and challenges of the existing information systems for the security audit according to the tools of the protection of information security, the study of the objects for the information security, search and collect the list of threats and vulnerabilities for all the objects including information security according to ISO standards, the preparation methods of decision-making on threats and vulnerabilities, and a core intellectual questionnaire for the experts to analyze the auditing environment. On the basis of implemented software and libraries of automatic generation of reports it was taken into account their conformity with international standards for information security (ISO 2700x).

In accordance with international and national standards information security developed by the system assumes the following:

- Definition of the objectives to ensure information security of the computer systems.
- Creation of an effective information security management system.
- Calculation of the aggregated detailed qualitative and quantitative indicators for the evaluation of the conformity information security objectives.
- Use of tools for information security and the evaluation of its current status.
- The use of safety management techniques to objectively assess the security information assets and to manage the information security of the company.

During analysis of a few commonly accepted international safety standards we have defined:

The role of each standard as well as the implementation of the Security in the general sense and according to the relationship with our system.

The standards and how it should be reflected in the knowledge base.

Specific structural elements and the relationship between them have been allocated where the content of the knowledge base was formed.

As a tool of storing received knowledge from standards we have selected storage technology into the database. In accordance with the ontology of the information security and the results obtained during analysis of standards we have developed model of objects and the relationships between them, the structure of the knowledge base as well as the mechanism for the rapid and effective addition of new instances for these objects. The database has a large number of meta-data on the area of information security as a whole and the data on a specific organization where there is an audit; with the help of the newly developed ontology of the IS and methodology of the standard’s analysis, namely extracting the basic concepts from them, the base is well-structured and easily managed.

References:


