Computer Modelling and New Technologies, 2011, Vol.15, No.4, 52–57
Transport and Telecommunication Institute, Lomonosov 1, LV-1019, Riga, Latvia

DEVELOPMENT OF DATABASE FOR EXPERT SYSTEMS OF INFORMATION SECURITY AUDITING

A. Bekezhanova[1], L. Atymtayeva[2]

[1]Kazakh-British Technical University
Department of Computer Engineering
Tole bi 59, 050000, Almaty, Kazakhstan
E-mail: ainagul.bs@gmail.com

[2]Kazakh-British Technical University
Department of Computer Engineering
Tole bi 59, 050000, Almaty, Kazakhstan
E-mail: l.atymtayeva@gmail.com

In this era of high technology, the information is involved in almost every aspect of human lives. Due to rapid growth of information technologies, came the need for increasing the security of information. Information security auditing plays key role in providing any organization's good security level. But, the security of information technologies is one of the difficult and comprehensive systems. The main problem lies in the data organization, collection and its processing methods. One of the solutions could be development of expert system that will reduce cost, speed up and facilitate the process of Information Security auditing. The valuable item in developing such system could be database development.

This paper presents the study of information security at international and national standards and guidelines for the management of IT, audit and IT-security (such as ISO 27001, COBIT 4.1 and ITIL V3) and the structure of database for expert systems of information security auditing.

Keywords: *information security, information security auditing, standards for auditing information security, expert systems, database, UML, Transact-SQL*

1. Introduction

The main goal of this study is based on the development of database of expert system, which will be fully audited information security and will be guided by the information that underlies the international standards ISO 27001, COBIT 4.1 and ITIL V3 [1].

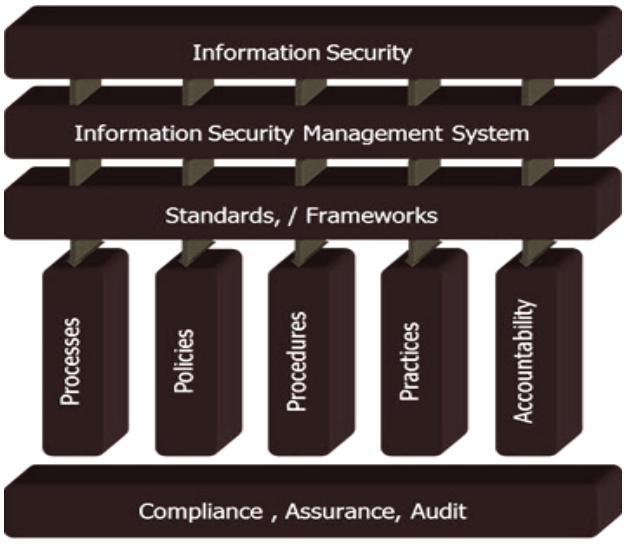

Figure 1. The structure of providing information security via standards/frameworks

The best global practices in the field of information security management are described in international standards that ensure compliance, assurance and audit of information security (see Fig. 1). We have also developed software implementation of database for expert systems of information security auditing in the language of queries Transact-SQL with the use of tool for developing relational database Microsoft SQL Server 2005 Management Studio Express.

2. Information Security Auditing

Firstly, let us focus your attention on the main concepts of information security.

Information security is defined by the absence of unacceptable risk of information leakage via technical channels, unauthorized and unintended effects on the data and other resources used in information systems (IS) [8].

Secondly, we should define the main characteristics of the audit of information security.

An audit is an independent examination of specific areas of organizational functioning. The objectives of the safety audit are [5]:

- The risk analysis;
- The assess the current level of protection of IS;
- The IS assessment of conformity with existing standards of Information Security;
- To develop recommendations for security mechanisms for IS.

For a professional approach to the issues of information security we should be guided by the regulating documents, such as standards. During the development of database for Expert Systems of information security auditing (ESISA) addressed the following international information security standards, such as ISO 27001, ITIL V3 and COBIT 4.1.

ISO 27001 was developed by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). ISO 27001 consists of 11 targets and monitoring mechanisms, which organize the protection of their information resources by establishing requirements for information security management system (ISMS).

On the basis of ITIL V3 laid process approach, consisting of seven volumes. It focuses on achieving business goals, analysing key performance indicators, as well as the resources expended to achieve those goals.

COBIT 4.1 consists of 34 high-level processes, which are aimed at business managers, IT managers and owners of business processes [7]. This approach is designed to extract maximum benefit from the use of information technology in organizations.

3. The Structure of the Expert Systems of Information Security Auditing

Expert System (ES) is an intellectual computer program that can give advice, counsel and analysis. The use of ES in the control and security management IS, and in the information security audit can facilitate the process of auditing [2]. The developed ES generates a report and recommendations based on the standards of information security and experts opinions. Go to the dignity of the ES also attribute to the possibility to describe the experience of information security professionals in a form accessible to the analysis of the rules If (condition) – Then (Corollary).

The structure ESISA consists of: a user interface, subsystem explanations, inference systems, the knowledge base and database. Structural elements of the expert system perform the following functions:

The user interface exists for direct interaction between ESISA and user, such as data entry and displays the results of the processed data.

The subsystem of explanations exists to clarify for the users the actions of the expert systems logic. The data from subsystem of explanations stored in database table – Recommendation.

The system of logical inference (SLI) carries a substitution of values from the database in the field of parcel If (condition) of the rules knowledge base and in the case of filling in all the parcels are ready to activate the processing rules, forming a conclusion in accordance with part Then (Investigation) regulations [6]. In the developing system SLI executes an application that created the language of logic programming Fril.

Knowledge Base (KB) is the core of the expert system. In the developing ES knowledge base is the main decision-making tool, the basic structure, which takes into account international experience and documents on the safety audit of IS, such as ISO 27001, ITIL V3 and the COBIT 4.1.

The relationship between the standards shown in Table 1, a fragment of which is shown below. Table1 is the source of the work [3].

Table 1.

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	CobiT 4.1 Control Objectives	CobiT IT Processes	ITIL V3 Reference
4.1 Assessing security risks	**4.0 Risk assessment and treatment**	• P09.4 Risk assessment	• P09 Manage IT risks	
4.2 Treating security risks			• P09 Manage IT risks	
5.1 Information security policy	**5.0 Security policy**			
5.1.1 Information security policy document		• P06.1 IT policy and control environment • P06.2 Enterprise IT risk and control framework • P06.3 IT policies management • P06.5 Communication of IT objectives and direction • DS5.2 IT security plan • DS5.3 Identity management • ME2.1 Monitoring of internal control framework	• P06 Communicate management aims and direction • DS5 Ensure systems security • ME2 Monitor and evaluate internal control	• SS 6.4 Organisational culture • ST 5.1 Managing communications and commitment • SO 3.6 Communications • SO 4.5 Access management • SD 4.6.4 Policies, principles, basic concepts • SD 4.6.5.1 Security controls (high-level coverage, not in detail)

There are a few questions from the established knowledge base, which is focused on the three categories of users: Govern – G, Admin – A, User – U (Table 2).

Table 2.

№	Question	Category
	Security Policy	
1	How often do changes/additions to the security policy in your company?	A
2	Have an occasion to inform outside parties documented information security policy of your company?	G
	Resource management	
3	Is there an inventory of all the important resources in your company?	G,A,U
4	Does your company support an inventory of all critical resources?	G,A

4. Development of Database

The database is a collection of organized data, stored in a computer memory. For creating, maintaining and sharing databases between many users used the set language and software tools, called a database management system (DBMS).

DBMS supports various methods of logical organization of data. The best-known data models are hierarchical, network and relational models. To develop ESISA database has been used a relational model. The basic concepts of relational databases are the normalization, keys, entities and relationships. The principles of normalization [4]:

- Each database table must not include repeated fields;
- Each table must have a unique identifier (primary key);
- Each primary key value must match the sufficient information about the type or nature of the object table;
- Change the values in the table should not affect the information in other fields.

Keys:

The key is a column or multiple columns to be added to the table and allow establishing a connection with the records in another table. There are two types of keys: primary and secondary. The primary key is used to relate a table to foreign keys in other tables. A foreign key indicates how to join with other tables. There are many types of relation, such as of “one-to-one,” “one-to-many” and “many-to-many”.

In the design process of ESISA determined the structure of a relational database, which contains 14 tables. Each table in DB consists of columns, data types, sizes and keys of table:

- ISO,
- ITIL,
- COBIT,
- Category,
- Questionnaire,
- Test,
- Report,
- Recommendation,
- TesterReport,
- Tester,
- Expert,
- Govern,
- Admin,
- Users.

For creating a database used development tools such as the Star UML and MS SQL 2005.

StarUML is a software modelling tool that supports the Unified Modelling Language (UML). Below are given the relationships between data tables in a database of association, direct association, generalization and composition in the development environment StarUML (Fig. 2).

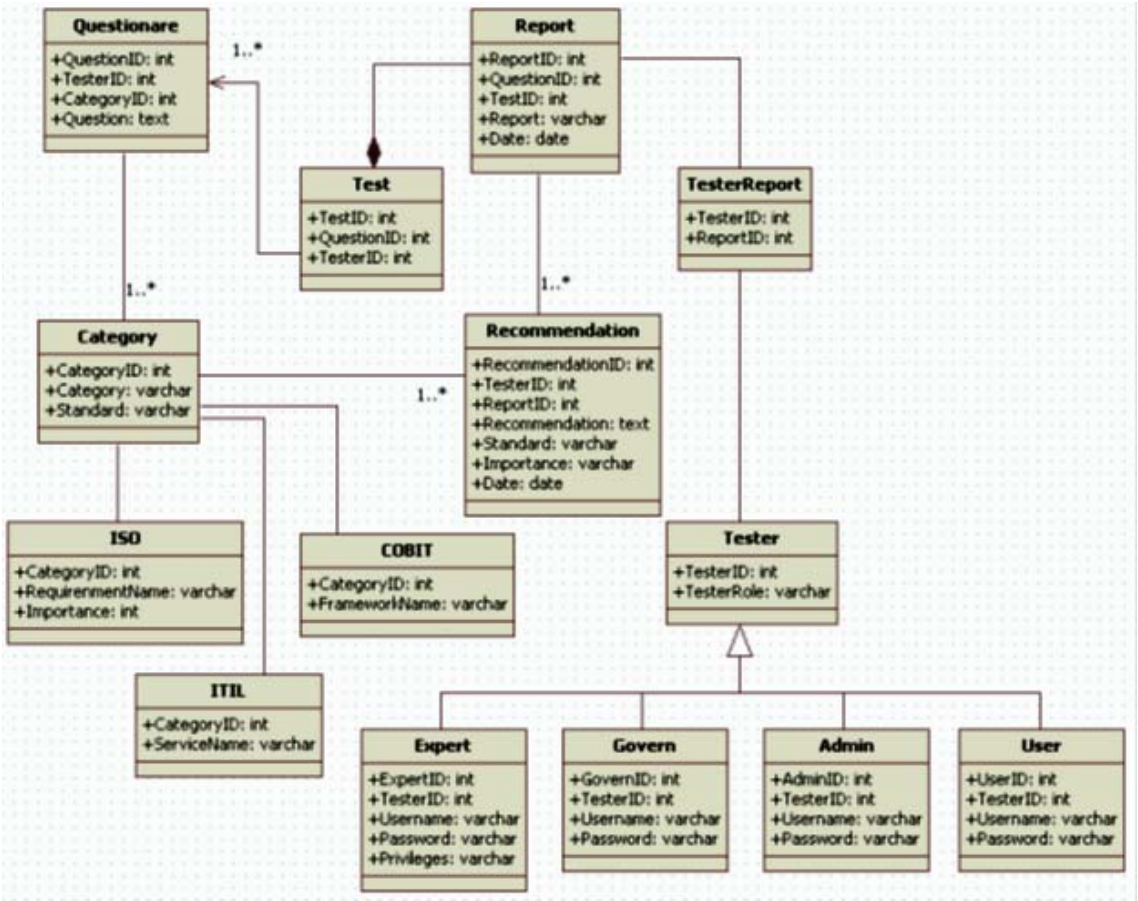

Figure 2. Model DB for ESISA in StarUML

Microsoft SQL Server is a DBMS developed by Microsoft. The primary query language used here is Transact-SQL. The advantage of SQL Server 2005 is the manageability, availability, scalability and security [4].

Let's consider the main points of application and work environment in MS SQL Server 2005.

First of all, for creating a database in MS SQL we use the operator to create a database: CREATE DATABASE databasename;

Then, the following queries are executed for creating tables and primary keys, which are defined for each table (queries for some tables are illustrated in the work area MS SQL Server 2005) (Fig. 3):

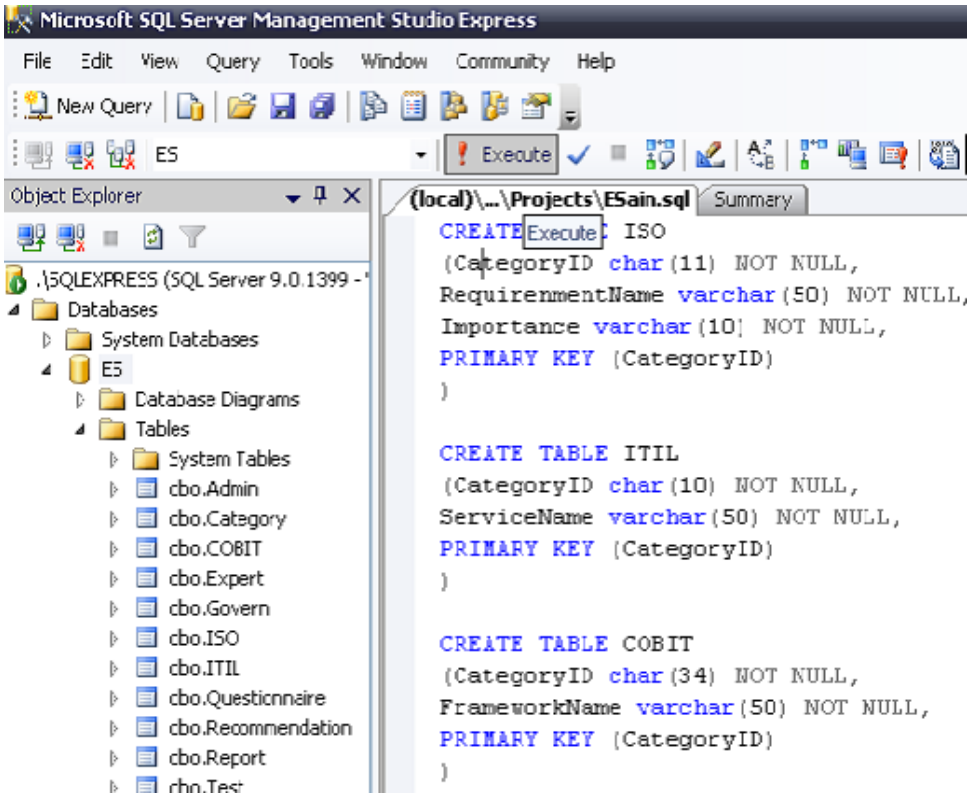

Figure 3. Queries for some DB tables in MS SQL Server 2005

The last step is filling tables with user's data. In MS SQL Server 2005 data filling is made through queries or manual entry of information.

5. Conclusions

This article focuses on the development of database for expert systems of information security auditing. The result of research is developed review and analysis of information security in accordance with international standards and guidelines for the management of IT, audit and IT-security, such as ISO27001, COBIT 4.1 and ITIL V3. Together, these standards contain requirements for information security for the creation, development and maintenance of information security management system.

The knowledge base for ESISA was created on the basis of the best international practices in the management of information security. It includes questions about the security of information and presented in the form of a questionnaire, the relevant standards of ISO27001, COBIT 4.1 and ITIL V3.

Structure of the database was designed on the Unified Modeling Language in the development environment StarUML. Software implementation is made in the queries language Transact-SQL with the use of Relational Database Management MS SQL Server 2005. Database tables have been designed according to knowledge base for ESISA.

Let us note that nowadays in Kazakhstan the research is conducted towards the development and implementation of expert system in security auditing. This framework of project named as "Development of intelligent systems for management and auditing of information security" is being financed by Ministry of education and science of Republic of Kazakhstan for 2012-2014 years.

In conclusion, we would like to note that the research results can be used in conjunction with the developing expert system in the auditing companies and any organizations interested in the proper functioning of safety systems.

References

1. Atymtayeva, L., Akzhalova, A., Kozhakhmet, K., Naizabayeva, L. (2011). Development of Intelligent Systems for Information Security Auditing and Management: Review and Assumptions Analysis. In Proceedings of the 5th International Conference on Application of Information and Communication Technologies, 12–14 October, 2011 (pp.87–91). Baku, Azerbaijan: Qafqaz University.
2. Giarratano, J.C., Riley, G.D. (2004). *Expert Systems: Principles and Programming*, 4th ed. Course Technology. Boston: PWS Publ. Co.
3. Appendix III—Mapping Cobi T 4.1 Control Objectives and ITIL V3 with ISO/IEC 27002. In Gary Hardy, Jimmy Heschl, Jim Clinch (Eds.), *A Management Briefing From ITGI and OGC* (pp. 90–128). Rolling Meadows, IL USA: IT Governance Institute.
4. Vieira, R. (2007). *Professional SQL Server 2005 programming*. USA, Hoboken, New Jersey: Wiley Publishing, Inc.
5. Clinch, J. *ITIL V3 and Information Security*. Clinch consulting (pp. 14–20). Retrieved May, 2009, from http://www.best-management-practice.com/gempdf/ITILV3_and_Information_Security_White_Paper_May09.pdf.
6. Safonov, V. O. (1992). *Expert systems – intelligent advisors of human experts.* St. Petersburg: Knowledge Publishers. (In Russian)
7. Cobit4.0 The newest evolution of control objectives for information and related technology. The world's leading IT control and Governance framework (2007). IT Governance Institute. http://win.dicrosta.it/Documenti/COBIT40-Brochure.pdf, http://www.itcinstitute.com/display.aspx?id=1208
8. Kiountouzis, E. A., Kokolakos, S.A. (1996). An analyst's view of IS security. In Sokratis Katsikas & Dimitris Gritzalis (Eds.), *Information systems security: facing the information society of the 21st century, IFIP SEC '96 Conference* (pp. 23–35). London: Chapman & Hall, Ltd.

Received on the 21st of December 2011