Expert systems for auditing management information systems

❖❖ GHEORGHE POPESCU ❖❖
❖❖CRISTINA RALUCA POPESCU❖❖
❖❖ VERONICA ADRIANA POPESCU ❖❖

Expert systems are built with the help of: specialised programming languages or expert system generators (shell). But this structure was reached after tens of years of work and research, because expert systems are nothing but pragmatic capitalisation of the results of research carried out in artificial intelligence and theory of knowledge.

Key words: *a*rtificial intelligence, audit, common sense, creativity, expert systems, expert system for auditing management information system, information technology, intelligence, intelligence systems, key risks, quality, security, theory of knowledge

I. Expert systems – pragmatic capitalisation of the results of research in artificial intelligence and theory of knowledge

Expert systems are the pragmatic ending of research in the fields of artificial intelligence and theory of knowledge**.** When they realised how difficult it is to build a machine with a similar behaviour to man's**,** specialists' concerns materialised in building expert systems – by restraining the knowledge scope to very narrow and well-defined fields that justify the professional judgement of human experts**.**

Advantages of Expert Systems

1. **Performance;**
2. **Reproducibility;**
3. **Efficiency;**

4. Consistency;

5. Documentation;

6. Timeliness - Fraud and/or errors can be prevented. Information is available sooner for decision making;

7. Breadth - The knowledge of multiple human experts can be combined to give a system more breadth that a single person is likely to achieve;

8. Entry barriers - Expert systems can help a firm create entry barriers for potential competitors;

9. Differentiation - In some cases, an expert system can differentiate a product or can be related to the focus of the firm.

Disadvantages of Expert Systems

1. **Common sense -** human experts have common sense, **but** we did not yet known **how to give** expert systems common sense.

2. Creativity - human experts can respond creatively to unusual situations, but expert systems cannot.

3. Learning - human experts automatically adapt to changing environments, **but** expert systems must be explicitly updated.

4. Sensory Experience - human experts have available to them a wide range of sensory experience, **but** expert systems are currently dependent on symbolic input.

5. Degradation - expert systems are not good at recognizing when no answer exists or when the problem is outside their area of expertise.

II. The specific of information systems audit

Establishing "an expert system for auditing management information system" - involves: identifying and modelling the experience of management information system expert auditor.

Information system audit represents a relatively recent and very modern concern, given the role of information technology, which strongly imposed in every sector of activity.

- Because using of information technology involves hardly negligible investments – these should be thoroughly justified.

- In addition, we deal with the risks related to an information technology which cannot be controlled.

Thus we can have in mind the key risks – specific to environments based on information technology:

- Reliance on the functioning capacities of information equipments and programmes;
- Accessibility of audit trail;
- Reducing the involvement of human factor;
- Incidental errors – systematic error;
- Unauthorised access;
- Losing of data;
- Reducing segregation of duties;
- Lack of traditional authorisation;
- Expertise necessary in information technology.

Risks are based on causes, generate damages and involve responsabilities:

1. causes are equally distributed among:

a) accidents and failures;

b) weak knowledge – computer being the target or the instrument;

c) errors.

2. damages are equally distributed among:

a) banks or financial and insurance services;

b) industry and agriculture;

c) transport, distribution and public services.

3. responsibilities are equally distributed among:

a) IT personnel;

b) non-IT personnel;

c) third parties external to the entity.

Assurance Standards, guidelines and procedures specific to information system audit - Auditing Standards Commission (S.U.A. - 1986) issued 11 standards on assurance specific to information system audit, which follow the pattern of the 10 general accepted auditing standards. **The role** of standards and guidelines is to assist the auditor in his activity, contributing to unitary interpretation of various and complex situations that information systems auditors may deal with.

ISACA – „ Information Systems Audit and Control Association "- On an international level, **Information Systems Audit and Control Association - ISACA**, issued its own standards, guidelines and procedures to assist the specialist, management personnel of the Association as well as the ***certified information systems auditors*** (**CISA –** *the Certified Information Systems Auditor*). At 1 May 2003 8 categories of standards were effective, comprising 12 standards and 24 guidelines. 6 working procedures were also available.

III. Procedures and techniques for auditing the main management information systems

In defining and auditing of information objectives:

- the general working method requires that information audit to be separated in three stages:

I) defining the objectives;

ii) conducting the audit (*collecting information, controls, analyses and reviews, preparation of the report*);

iii)subsequent operations (*checking the application of provided recommendations, checking the application of maintenance*).

The following are procedures and techniques commonly used in the audit activity:

a. Analytical procedures;
b. Testing or sampling;
c. Debating groups;
d. Interviews;
e. Questionnaires;
f. Documentary examination;
g. Factual examination.

The following are specific procedures and techniques used in the audit activity:

- Documenting the information system, which deals with**:**

- information system and computerised controls,
- reviewing the procedures which are the compilations basis,
- testing and reviewing system transactions;

- Assessing the effectiveness of controls;

- Computer Assisted Audit Techniques (CAAT)**.**

The stages of information systems audit engagement consist of:

- Accepting the engagement**;**
- Planning the audit mission**;**
- Collecting and assessing the audit evidence**;**
- Finalising the mission**.**

The solution adopted for establishing an expert system for management information system audit consisted of:

- splitting the management information systems audit in sub-fields,
- identifying sub-problems which may be solved on an independent basis,
- trying to subsequently reintegrate these problems in a unique structure of knowledge basis.

The main difficulty in modelling and formalising knowledge in this field is the complexity of the information systems audit, which requires performing of some expertises that use knowledge from separate or interrelated fields of knowledge (technical, information, communications, financial, fiscal, juridical, accounting, commercial, management, human resources).

IV. Model of an expert system for auditing management information systems

Information system also involves the existence of specific elements, such as:

- technical and communication resources represented by computers and data transmission media**;**
- software resources represented by operation systems and applications**;**
- human resources represented by personnel specialised in creating**,** managing and maintaining applications or in obtaining**,** processing and interpreting information**;**
- data necessary for processing**.**

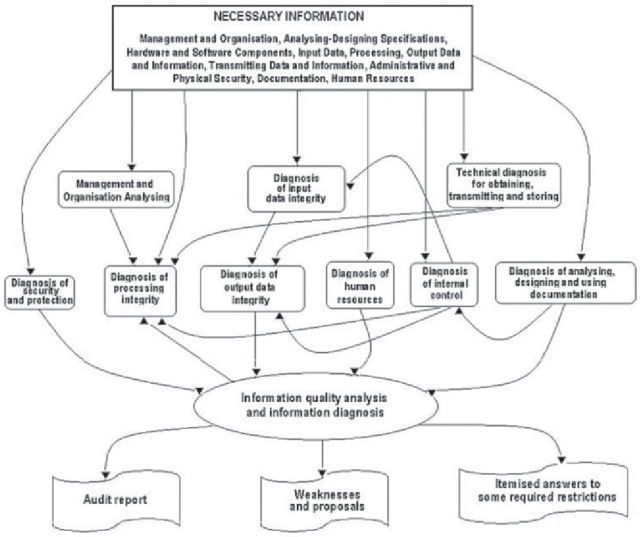
I have also identified the subfields of management information systems audit activity, for which independently explored knowledge basis may be built, regarding:

- diagnosis of input data integrity**;**
- technical diagnosis for obtaining**,** transmitting and storing**;**
- diagnosis of processing integrity**;**
- diagnosis of internal control;
- diagnosis of security and protection**;**
- diagnosis of output data integrity**;**
- diagnosis of human resources**;**
- diagnosis of analysing**,** designing and using documentation**;**

- information quality analysis and information diagnosis.

Sub-fields of management information systems audit activity – Starting from **necessary information,** like as: management and organisation, analysing-designing specifications, hardware and software components, input data, processing, output data and information, transmitting data and information, administrative and physical security, documentation, human resources, **we diagnosis** all these elements, obtaining: audit report, weaknesses and proposals, itemised answers to some required restrictions.

Figure nr. 1 – *Sub-fields of management information systems audit activity*



[1] Some of these are taken from Carol E. Brown şi Daniel E. O'Leary – „Introduction to Artificial Intelligence and Expert Systems", 1993.

BIBLIOGRAPHY

1. **Carol E. Brown şi Daniel E. O'Leary** – *„Introduction to Artificial Intelligence and Expert Systems"*, 1993.

2. **Barr, A., Feigenbaum, E.A**. – *„The Handbook of Artificial Intelligence"*, Heuris Tech Press, New Zork, 1981;

3. **Munteanu, A.** – *„Accounting Information Systems Audit"*, Ed. Polirom, 2001;

4. **Popescu, Gh**. – *„Internal Control and Financial Audit Procedures"*, Ed. Gestiunea, Bucureşti, 1997;

5. **Popescu, V.** – *„Expert Systems for Auditing Management Information Systems"*, Ed. Gestiunea, Bucureşti, 2006.