DECISION MODELING BASED APPROACH TO THE BS 7799 DEPLOYMENT

Tomas Feglar
Vondrousova 1199, 163 00 Prague 6, Czech Republic
feglar@czn.cz

Keywords: BS 7799, Decision Modeling, AHP hierarchy, resource allocation, risk driven, hypotheses.

Summary: *The paper describes decision modeling based approach to the BS 7799 deployment. First we briefly introduce why BS 7799 is important in the age of Electronic Commerce. Then we identify limitations that characterize risk driven approach to the BS 7799 deployment. We argue that these limitations can be overcome with decision modeling based approach using AHP hierarchy. This hierarchy includes two types of criteria levels – static and dynamic. Decision making model that uses this hierarchy includes three particular processes: BS 7799 Deployment Modeling, Risk Driven Countermeasure (RDC) generation and Human Resource Allocation Alternatives (HRAA) generation process. Our approach is supported with three powerful tools to achieve appropriate quality of decisions and performance. BS 7799 Deployment Modeling uses EC 2000, RDC process uses CRAMM and HRAA generation is based on GUHA. Proposed decision modeling approach controls interactions between all three tools and generates final objective – optimal BS 7799 deployment.*

1. Introduction

More and more companies understand that decision making becomes more a science than a art. Management of these companies uses exact methods like AHP and ANP /10,12/ as a framework for all strategic business decisions. At the same time more and more companies become dependent on information systems that introduce additional risks that can seriously damage core business activities. Security Standard BS 7799 was developed to help companies to minimize these risks. BS 7799 deployment becomes one of the strategic business decisions. This deployment is currently based on risk driven approach that is different from a framework usually used for decision making.

We are going to present new decision modeling based approach to the BS 7799 deployment. This approach does not replace risk driven approach but rather enhances it in two directions.

The basement of our approach is AHP Hierarchy structure with “static” criteria that relate to BS 7799 and with “dynamic” criteria that are synthesized on the base of risk analysis. This direction allows top management directly participates on BS 7799 deployment by the way it uses for other decision making situations.

The second directions takes into account a fact that companies store information about human resources and contracts in their databases. We introduce new concept of human resource allocation alternatives using hypotheses generation.

2. BS 7799 from Viewpoint of Decision Modeling

The security of information – its confidentiality, integrity and availability – is a key management concern in the modern, electronic business world. This trend becomes especially important in Europe where the introduction of Economic and Monetary Union accelerates Electronic Commerce.

Successful organizations depend on accurate, secure and accessible information to make the myriad decisions, which shape their business and maintain their competitive edge.
BS 7799 is a British Standard, which was developed as a result of industry, government and commerce demand for a common framework to enable companies to develop, implement and measure effective security management practice and to provide confidence in inter-company trading. Last version of this standard was accepted as ISO standard in the Y 2000 and has two parts. BS 7799 – 1 (BS ISO/IEC 17799) Information technology – Code of practice for information security management is the first part. BS 7799 – 2 Information Security Management Systems is the second part (BS 7799, 2000).

It is strongly recommended to deploy BS 7799 on the base of security requirements that are identified by a methodical assessment of security risks. One of the leading risk assessment methods is CRAMM – Central Computer and Telecommunication Agency (CCTA) Risk Analysis and Management Method (CCTA, 1991). CRAMM is very powerful method especially for design and development security strategy based on risk driven countermeasures. There are also two serious limitations for CRAMM application:

- CRAMM reports are very detailed and very difficult for understanding by the top management that is responsible for strategic business decisions. Top management in commercial companies needs for its decision more transparent security presentation. Categories of Efficiency, Internal Assurance, Customer Trust or Business Partner Trust are much more useful than details about implementation of particular countermeasure.
- CRAMM reports include a lot of recommendations concerning countermeasures and responsibilities. It is useful for a design of an overall company security profile. This profile is also difficult for understanding by the top management that prefers to have information about staff responsible for security issues and about cost of external contracts that cover security issues beyond the scope of company's manpower or skill.

We suggest overcoming risk driven deployment limitations of BS 7799 with new approach that is based on decision modeling and human resource allocation alternatives generation.

Decision modeling principles are based on AHP theory founded by T.L. Saaty (Saaty, 2000). They are briefly explained in the third part. Part 4 relates to the interaction between three fundamental processes that we combine during modeling of BS 7799 deployment. Core process is BS 7799 Deployment modeling that interacts with two supplemental processes; Risk driven countermeasure generation and Human resource allocation alternatives generation. Part 5 explains principles of resource allocation based on General Unary Hypothesis Automation (GUHA) method (Hajek,, Havel, and Chytil,1966). .

3. AHP Hierarchy for a BS 7799 Optimal Deployment

Everybody who uses AHP for modeling a decision problem first defines the situation carefully including as many relevant details as possible. Then he structures it into hierarchy of levels of detail. The highest level will be overall objective of a BS 7799 Optimal Deployment (Fig. 1). Lower hierarchical levels include:

- Strategic criteria of a Decision Making Model (DMM). Hierarchical levels L1, L2 and L3 describe "static" criteria that are easily understandable for the top management. L1 criteria serve for finding of a compromise between "internal motivation" (Efficiency, Internal Assurance) and "External Image" (Customer Trust, Business Partner Trust). L2 and L3 levels relate to the BS 7799 structuring (see Table 1).

SC Ide	Security Category Description
SC - 1	Management System Requirements
SC - 2	Security Policy
SC - 3	Security Organization
SC - 4	Assets Classification and Control
SC - 5	Personnel Security
SC - 6	Physical and Environmental Security
SC - 7	Communications and Operations
SC - 8	Access Control
SC - 9	System Development and Maintenance
SC - 10	Business Continuity Management
SC - 11	Compliance

Table 1. List of Security Categories in BS 7799

- Operational criteria of a DMM. Hierarchical levels L4 and L5 describe “dynamic” criteria that depend on Risks and Responsibility Assignment. Risks and Responsibilities become known only on the base of the Risk Analysis Process. “Dynamic” criteria are difficult to understand without very good information technology security background. L4 criteria describe countermeasure groups (CG). Each Security Category (L3) can be represented as a cluster of countermeasure groups. Table 2 includes a sample of countermeasure groups and countermeasure sub-groups (CSG) for Security Category 10 (Business Continuity Management). L5 Criteria describe relationships between particular responsibility and countermeasure groups (sub-groups). Table 3 includes a sample of a Human Resource (HR) responsibility.

C Identifier.	Countermeasure Description
CG - 1	Business Continuity Plans should be produced
CSG - 1 - 1	Managed BCP Process
CSG - 1 - 2	Maintain the Framework of the Business Continuity Plan
CG - 2	The Business Continuity Strategy should be based on a Risk Assessment
CSG - 2 - 1	The risks that can cause interruptions to the business process to be defined
CSG - 2 - 2	An Impact assessment to be conducted
CSG - 2 - 3	The risk assessment to cover all business processes
CG - 3	Business Continuity Plans should be subject to regular tests
CSG - 3 - 1	The Types of testing to be conducted to be specified
CSG - 3 - 2	Plans to be updated to reflect and lessons learned from the tests

Table 2. Sample of Countermeasure Groups within SC - 10

C Identifier.	HR Responsibility
CG - 1	System Manager, Operations Manager, Network Manager, Building Manager
CG - 2	Operations Manager
CG - 3	Operations Manager

Table 3. Sample of Human Resource Responsibility

- Hypotheses about HR Allocation Alternatives. At the bottom of our hierarchy we can see four Allocation Scenarios (AS). Each AS represents security concept with some kind of preference. Scenario 1 prefers BS 7799 deployment strongly on the base of internal staff (company employees). Scenario 4 prefers to cover all BS 7799 deployment effort within one contract with Computer Services Business Center (CSBC). Real situation requires a combination of scenarios in dependency on final structure of the levels L4 and L5. HR Allocation Alternatives are generated on the database data (HR pool, contracts, costs) with respect of a particular AS. The generation process is hypotheses driven.

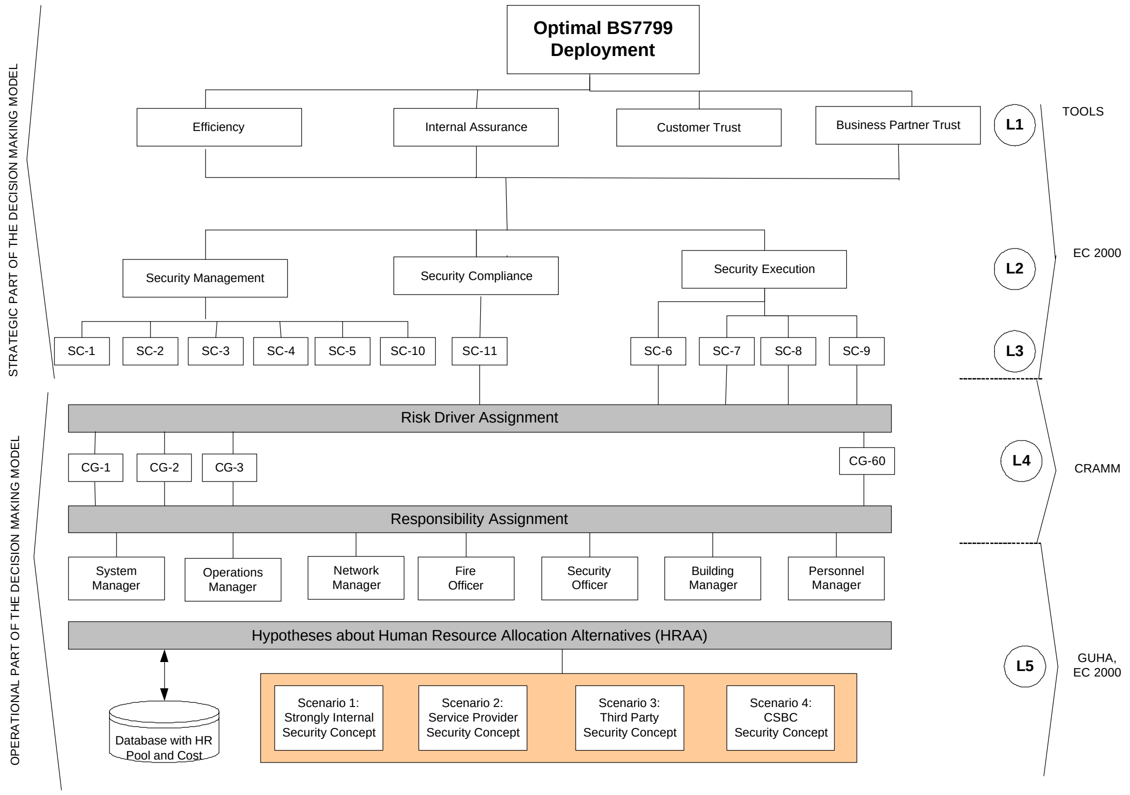

STRATEGIC PART OF THE DECISION MAKING MODEL
OPERATIONAL PART OF THE DECISION MAKING MODEL
Optimal BS7799 Deployment
Efficiency
Internal Assurance
Customer Trust
Business Partner Trust
Security Management
Security Compliance
Security Execution
SC-1
SC-2
SC-3
SC-4
SC-5
SC-10
SC-11
SC-6
SC-7
SC-8
SC-9
Risk Driver Assignment
CG-1
CG-2
CG-3
CG-60
Responsibility Assignment
System Manager
Operations Manager
Network Manager
Fire Officer
Security Officer
Building Manager
Personnel Manager
Hypotheses about Human Resource Allocation Alternatives (HRAA)
Database with HR Pool and Cost
Scenario 1: Strongly Internal Security Concept
Scenario 2: Service Provider Security Concept
Scenario 3: Third Party Security Concept
Scenario 4: CSBC Security Concept
L1
L2
L3
L4
L5
TOOLS
EC 2000
CRAMM
GUHA, EC 2000

Fig. 1 AHP Hierarchy for BS 7799 Security Package Design

Decision process that uses hierarchy just described (Fig. 1) requires high expertise at least in the' areas of decision making, risk analysis and information security. It is not easy to put together so different experts. We overcome this problem using three powerful tools:

- Expert Choice 2000 (EC 2000) for a development of the AHP hierarchy and for BS 7799 Decision modeling (Expert Choice, 2000).
- CRAMM for dynamic creation of the criteria at the levels L4 and L5 (CCTA, 1991)
- GUHA for Human Resource Allocation Alternatives (HRAA) hypotheses generation (GUHA).

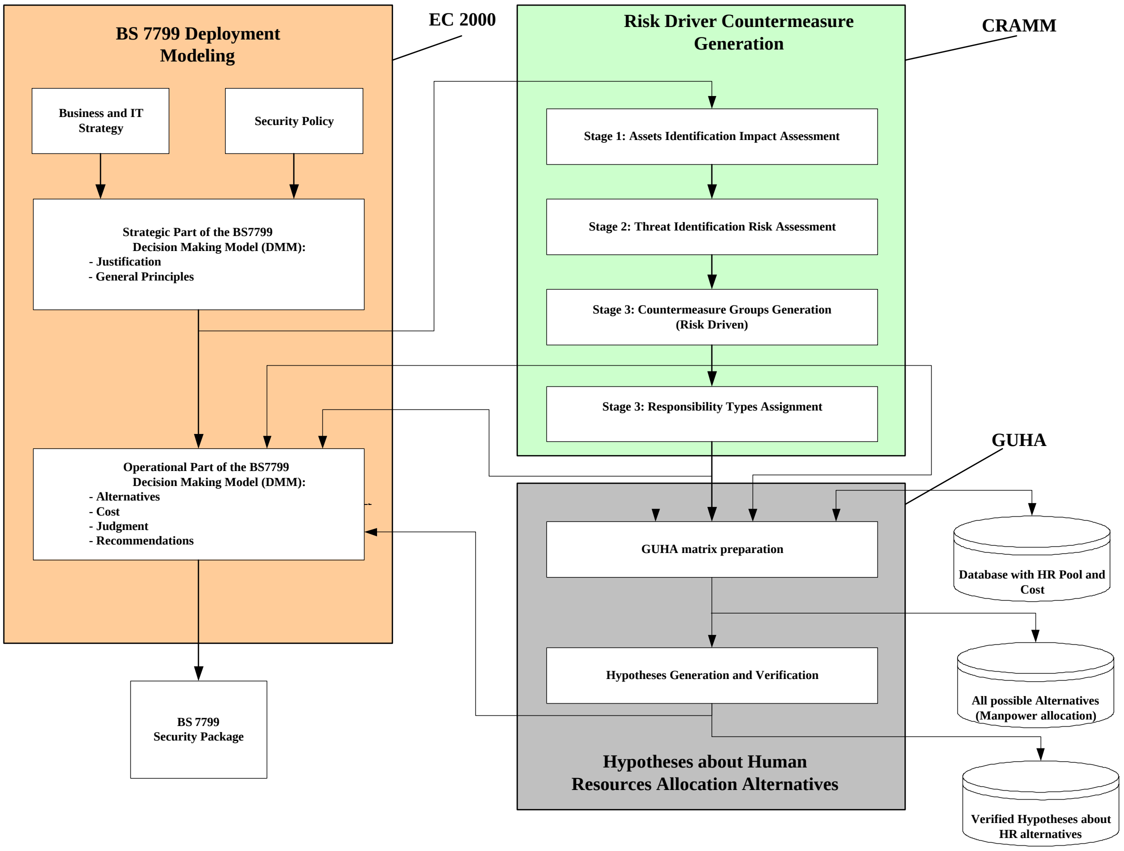
4. Key processes applied for BS 7799 Deployment modeling

Smart functionality of our model requires careful planning of key processes that interact each other (Fig. 2).

The first process is the BS 7799 Deployment Modeling. This process includes all steps necessary for building of the AHP hierarchy. Criteria levels L1, L2 and L3 are built on the base of a Business and IT Strategy and Security Policy. Bottom criteria levels – L4 and L5 are synthesized on the base of outputs from the Risk Driven Generation process. Alternatives are synthesized on the base of outputs from the HRAA Generation process. This process is supported by EC 2000.

The second process is the Risk Driven Countermeasure Generation process. It includes all steps that are necessary for creation of a set of risk driven countermeasures and for responsibility types assignment. This process is supported by CRAMM.

The third process is the Human Resource Allocation Alternatives (HRAA) Generation process. This process is supported by GUHA (see next part).



BS 7799 Deployment Modeling
EC 2000
Risk Driver Countermeasure Generation
CRAMM
Business and IT Strategy
Security Policy
Stage 1: Assets Identification Impact Assessment
Stage 2: Threat Identification Risk Assessment
Strategic Part of the BS7799 Decision Making Model (DMM):
- Justification
- General Principles
Stage 3: Countermeasure Groups Generation (Risk Driven)
Stage 3: Responsibility Types Assignment
GUHA
Operational Part of the BS7799 Decision Making Model (DMM):
- Alternatives
- Cost
- Judgment
- Recommendations
GUHA matrix preparation
Database with HR Pool and Cost
Hypotheses Generation and Verification
All possible Alternatives (Manpower allocation)
BS 7799 Security Package
Hypotheses about Human Resources Allocation Alternatives
Verified Hypotheses about HR alternatives

Fig. 2 BS 7799 Decision Making Model and its Environment

5. Human Resource Allocation Alternatives based on GUHA

5.1. GUHA and Decision Making

GUHA is a method originated in Prague (in Czechoslovak Academy of Science) in mid-sixties (Hajek, Havel, and Chytil, 1966). Its main principle is let the computer generate an evaluate all hypotheses that may be interesting from the point of view of the given data and the studied or decision oriented problem. GUHA is now important research direction in he European grant EC COST 274 (TARSKI – Theory and Applications of Relational Structures as Knowledge Instruments). Special attention is given to data mining (Hajek, 2001; Hajek, Feglar, Rauch and Coufal, 2002) and decision-making (Feglar, 2001; Feglar, 2002).

Starting notion of the method is an object. Object has properties expressed by couples <Attribute (A), Value (V)>. In order to make reasonable knowledge discovery we need to have a set of objects of the same kind (the same set of attributes) that differ in values.

To explain our understanding of relationship between GUHA principles and decision making we start with the nice example described by T.L. Saaty in the chapter 2 of (Saaty, 2001). Decision problem deals with "Satisfaction with House" (Fig. 3).

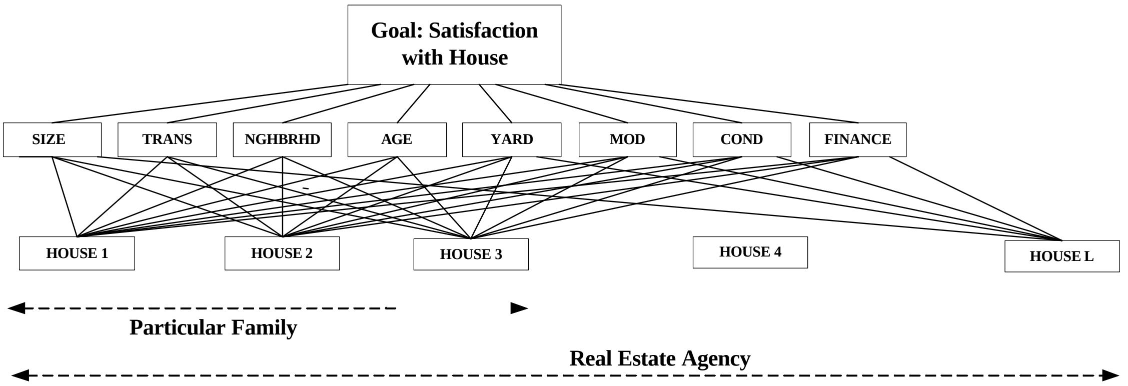


Fig.3. Decision Making Problem and two Perspectives: Particular Family and Real Estate Agency

From perspective of one particular family there is not very difficult to design and apply AHP hierarchy because number of alternatives is known and limited to a few houses. We try to replace particular family with Real Estate Agency that realizes a hundred of houses transaction per year and all data about these transactions are stored in a database (Table 4). Houses HOUSE 1, .., HOUSE L are objects in GUHA sense. The couples <SIZE,4>, <TRANS,5> fix properties of a particular house. The couples <C_OCCUP, worker>, <C_AGE, 30> fix properties of a particular customer who bought house. Some houses were not bought yet (HOUSE 3). Full description of attributes and their values is in the Table 5.

Attributes \ House ID	**SIZE**	**TRANS**	**NGHBRHD**	**AGE**	**YARD**	**MOD**	**COND**	**FINANCE**	**C. OCCOP.**	**C. AGE**	**C. SAT**
HOUSE 1	4	5	rush	5	500	-	Approp.	Loan	Worker	30	M
HOUSE 2									Manager	40	H
HOUSE 3									-	-	
HOUSE 4											
.											
HOUSE L	6	60	village	20	5000	Internet	Very Good	cash	Scientist	55	H

Table 4. Real Estate Agency Database

Attributes	Description	Distinct Values	Examples of values
SIZE	Number of rooms	15	3, 4 …
TRANS	Distance to the bus station	10	< 5 min; 10 min.,…
NGHBRHD	Neighborhood	15	rush, village, ….
AGE	Age of House	30	new, 2 yours, …
YARD	Yard Space	20	500 m2, 750 m2,…
MOD	Modern Facilities	20	dish washers, Internet
COND	General Condition	9	Excellent, Very good,…
FINANCE	Financing	5	Loan, cash
C. OCCUP.	Customer Occupation	50	Manager, Scientist
C.AGE	Customer Age	7	< 20 years, <21, 30>
C. SAT	Customer Satisfaction	5	L-Low, M-Medium, H-High

Table5. Attributes and Values in the Real Estate Agency Database

The aim of GUHA method is to generate hypotheses on relations among properties of the objects that are in some sense interesting. This generation is processed systematically; the machine generates in some sense all possible hypotheses and collects the interesting ones. The hypotheses are generally composed of two parts: from antecedent and a succedent.. So-called generalized quantifier (~) ties the antecedent (elementary conjunctions on the left site of the expression (1)) and succedent (elementary conjunctions on the right site of the expression (1)) together.

$$\text{NGHBRHD(village)} \wedge \text{MOD(Internet)} \wedge \text{COND(Excellent)} \wedge \text{COND(Very Good)} \sim \qquad (1)$$
$$\sim \text{C\_OCCUP(Scientist)} \wedge \text{C\_AGE(<51, 60>)}$$

GUHA supports various types of quantifiers. Applying implicational quantifier like $=>_{90\%}$ in the expression (1) we obtain semantic interpretation of hypothesis as follows “At least 90% of houses in the village equipped with Internet and having Excellent or Very Good conditions are bought by scientists in the age between 50 and 60 years”.

Positive verification of this hypothesis over Real Estate Agency database let this agency sufficiently improve decision model in the Fig. 3 for a particular customer’s group. Such improvement can be interpreted as some kind of optimization of houses allocation to the particular group of customers.
Verification process for each particular hypothesis produces frequency table called ff-table with four frequencies a,b,c,d.

	S	lS
A	a	b
lA	c	d

Table 6. ff-table

5.2. Hypotheses and Resource Allocation

GUHA can effectively support the Operational Part of the DMM (Fig. 2). It has access to all information about Human Resources (Employees), Contracts (Service Providers, Third Parties, CSBC) and Costs. All these data are converted by GUHA into the tables like Table 7.

Manpower	SC - 10							COST	COST_R
	CG-1		CG-2			CG-3			
	CSG-1-1	CSG-1-2	CSG-2-1	CSG-2-2	CSG-2-3	CSG-3-1	CSG-3-2		
M1 (m1,m2,m3,m4)	P	A	G	G	A	P	P	35	0.1458
M2 (m1,m2,m3,m4)	G	G	G	VG	G	A	A	50	0.208
M3 (m1,m2,m3,m4)	G	VG	VG	E	VG	G	G	75	0.3125
M4 (m1,m2,m3,m4)	VG	VG	E	E	VG	VG	VG	80	0.3333
								? =240	

Table 7. Manpower Allocation Alternatives for Security Category 10 (Business Continuity Management) – Fragment.

Various alternatives of resources are represented by table rows. Each alternative M has four items. Item m1 relates to the manpower covered strongly by internal human resources (employees) – see Scenario 1 in the Fig. 1. Item m2 relates to the manpower covered by service provider staff on the contract base – see Scenario 2 in the Fig. 1. Item m3 relates to the manpower covered by third party staff on the contract base – see Scenario 3 in the Fig. 1. Item m4 relates to the manpower covered by CBSC staff on the contract base – see Scenario 4 in the Fig. 1.

Couples <CSG-1-1, P>, … , <CSG-3-2,VG> reflect degree of satisfaction (see Table 8). Couples <COST,35>, …, <COST,80> reflect cost of a particular alternative. Couples <COST_R, 0.1458>, .., <COST_R,0.3333> reflect relative costs.

Degree of satisfaction with BS 7799 quality of deployment	Symbolic Value	Numeric Value
Excellent	E	9
Very Good	VG	7
Good	G	5
Appropriate	A	4
Poor	P	2
Very Poor	VP	1

Table8. Degrees of Satisfaction with the BS 7799 Quality of Deployment

Number of manpower alternatives and number of attributes may be large enough in real situations (50 and more alternatives, 20 and more attributes and within each attribute 6 couples (when we apply degree of resolution in accordance with Table 8). We also remember that BS 7799 has 11 security categories – Table 7 illustrates only fragment of table for SC 10.

It has no sense put all these manpower alternatives into our DMM (Fig. 1) if we are able to exclude "bad" alternatives on the base of verified hypotheses. Hypotheses generation and verification process will include:

- A combination of couples reflecting degree of satisfaction with BS 7799 quality of deployment (see Table 7) as Antecedent (A);
- A couple <COST_R,Value> as Succedent (S) (where Value relates to the budget limitation)
- Implicational quantifier between Antecedent and Succedent.

ff-table used for human resource allocation alternatives on the base of manpower allocation testing and verification can be interpreted as follows.

	B	**lB**
A	a	b
lA	c	d

Table 9. ff-table for Manpower Allocation Testing and Verification

a- Number of alternatives where:
- All countermeasure groups achieve requested quality (degree of satisfaction) – Antecedent A is TRUE
- Cost (COST) is equal or less then available budget - Succedent S is TRUE

b- Number of alternatives where:
- All countermeasure groups achieve requested quality – Antecedent A is TRUE
- Cost is higher then available budget – Succedent S is FALSE

c- Number of alternatives where:
- Not all countermeasure groups achieve requested quality – Antecedent A is FALSE
- Cost is equal or less then available budget – Succedent S is TRUE

Application of principles described above for pre-processing of all potential human resource allocation alternatives let us return to the DMM only alternatives that are near to optimal (see Fig. 2).

6. Discussion and Future work

Information security was understood as something mysterious for a long time. Last decade changed significantly overall picture. BS 7799 allows including information security as integral part of business processes. This new opportunity requires changes in the area of decision making. The approach presented in this paper completely covers three most critical parts of the BS 7799 deployment. AHP hierarchy including static and dynamic set of criteria is the core of decision making modeling.

Dynamic criteria are generated in dependency on risks – risk driven countermeasure generation is the second part. Finally human resource allocation alternatives are pre-prepared using automatic hypotheses generation and testing.

Topics for further research include:
- Verification of the approach at least on two different types of companies
- More detailed research of human resource allocation in dependency on various scenarios.

Acknowledgements

Research described in this paper is the subject of Czech participation in the EU COST 274 (TARSKI). Support of this grant is acknowledged.

References

BS 7799 (2000), (URL) http://www.c-cure.org/bs7799.htm

CCTA. (1991) The CCTA Risk Analysis and Management Method (CRAMM), Users Guide, CCTA IT Security and Privacy Group, London, 245 p.

Expert Choice (2000), (URL) www.expertchoice.com

Feglar,T. (2001) : “The GUHA Architecture”, *Proceedings of Relmics 6*, Tilburg (The Nederland), pp. 358 – 364.

Feglar,T.(2002): “Modeling of an engine based approach to decision support”. *Proceedings Advances in Databases and Information Systems ADBIS 2002*, September 8-11, Vol. 2, pp. 98 – 107.

GUHA, (URL) http://www.uivt.cas.cz/ics/software.htm

Hajek,P., Havel,I., Chytil,M.(1966): The GUHA method of automatic hypotheses determination, Computing 1, pp.293 – 308.

Hajek,P. (2001): “Relations in GUHA style data mining”. *Proceedings of Relmics 6*, Tilburg (The Nederland), pp.91 – 96.

Hajek,P., Feglar,T., Rauch,J., Coufal,D. (2002): The GUHA method, data preprocessing and mining. *Proceedings of International Workshop on Database Technologies for Data Mining*, Prague, April.

Saaty,T.L (2000).: “*Fundamentals of Decision Making and Priority Theory with The Analytic Hierarchy Process”*, Vol. VI of the AHP series, RWS Publications, Pittsburg, ISBN 0-9620317-6-3

Saaty,T.L.(1999): “*Decision Making for Leaders. The Analytic Hierarchy Process for Decisions in a Complex World”*, RWS Publications, Pittsburg, ISBN 0-9620317-8-X

Saaty,T.L. (2001): “*Decision Making with Dependences and Feedback”*. The Analytic Network Process, RWS Publications, Pittsburg, ISBN 0-9620317-9-8.