Early requirements engineering for e-customs decision support: Assessing overlap in mental models

Brigitte Burgemeestre, Jianwei Liu, Joris Hulstijn, Yao-Hua Tan

Faculty of Economics and Business Administration,
Vrije Universiteit, Amsterdam,
{cburgemeestre, jliu, jhulstijn, ytan}@feweb.vu.nl

Abstract. Developing decision support systems is a complex process. It involves stakeholders with diverging interpretations of the task and domain. In this paper, we propose to use ontology mapping to make a detailed analysis of the overlaps and differences between mental models of stakeholders. The technique is applied to an extensive case study about EU customs regulations. Companies which can demonstrate to be 'in control' of the safety and security in the supply chain, may become 'Authorized Economic Operator' (AEO), and avoid inspections by customs. We focus on a decision support tool, AEO Digiscan, developed to assist companies with an AEO self-assessment. We compared the mental models of customs officials, with mental models of the developers of the tool. The results highlight important differences in the interpretation of the new regulations, which will lead to adaptations of the tool.

Keywords: e-government, shared mental models, decision support systems

1 Introduction

The creation, implementation and enforcement of legislation are complex processes that involve a large amount of people, parties and disciplines [8]. In this paper we discuss a decision support system to assist in such a complex regulatory environment. The European Union has drafted new customs legislation intended to make supply chains more secure. Trustworthy companies are certified by customs authorities to become 'Authorized Economic Operator' (AEO[1] [2]) and benefit from reduced customs inspections [1]. The AEO legislation has to be implemented by national customs, enforced by regional customs authorities and understood and applied by businesses. As a result, we observe the introduction of several decision support systems which try to support these tasks. To align the tasks of the stakeholders in the certification process, such decision support systems have to take complex stakeholder characteristics into account.

The phase of early requirements engineering aims to analyze stakeholder interests and how they might be addressed or compromised by system requirements [23] [5]. A well known approach to early requirements engineering is the *i** framework [23] which proposes an actor-oriented approach, based on the goals and intentions of an actor. It consists of two main modeling components: the Strategic Dependency (SD) model contains dependency relationships among actors in an organizational context, while the Strategic Rationale (SR) model describes stakeholder interests and

[1] http://www.douane.nl/zakelijk/aeo/en
[2] http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security

Dagstuhl Seminar Proceedings 09121
Normative Multi-Agent Systems
http://drops.dagstuhl.de/opus/volltexte/2009/1916

concerns, and how they are addressed by the system. An important issue that is not addressed by early requirements methods like *i**, is the existence of overlap or differences in the interpretations of the various stakeholders. Much work in requirements engineering implicitly assumes that mental models of the task and domain are shared among stakeholders. In practice however, this assumption is not always warranted. Overlap in task-specific knowledge structures or having a 'shared mental model' is argued to have a positive influence on performance and effectiveness in collaborative situations [8] [4] [14]. We argue therefore that early requirements engineering should involve identification of the differences and similarities that exists among the mental models of the stakeholders. With the differences clarified, the stakeholders become aware about each other's mental model constructs, which they in turn can use to align their approaches. Unlike some of the empirical work on shared mental models, however, we are not satisfied with mere lists of differences. Instead we propose to use conceptual models in the form of ontologies, in the sense of CommonKADS [17], as well as ontology mapping techniques, to detect divergent or synonymous concepts in two or more ontologies in a systematic and precise way.

The need to analyze mental models of stakeholders is particularly important in the development of innovative e-government solutions. E-government solutions aim to modernize and reorganize the public sector though new methods of governmental business [15]. Examples are one-stop government shops, public-private partnerships or outsourcing to the customer [20]. Especially in public-private partnerships, multiple parties are involved with different interests and backgrounds, leading to different interpretations. Moreover, the legislation involved in e-government solutions is often new or still evolving, which makes its interpretation also difficult for the regulator. This suggests that the regulator should be modeled like any other actor, with its own specific interests and beliefs about the task and domain. The idea to treat the regulator as any other actor is advocated by Boella et al [2]. Using Normative Multiagent Systems (NMAS), they analyze various regulative environments and study the interactive 'games' which agents play to determine whether it is in their interest to obey a norm or not, and for regulators, whether to enforce a norm or not, depending on the expected behavior of the other agents. For such games, the actual norms do not matter much; what matters are the perceptions agents have of the other agents' mental models of the norms.

In this paper we discuss the initial results of our research on assessing overlap in mental models. The research method is qualitative and empirical. We focus on a decision support system called 'AEO Digiscan' that supports companies in performing the self-assessment, which is required to obtain AEO certification. We have conducted interviews with experts from both the Dutch Customs and Tax Administration (DTCA) and from the consultancy firm Deloitte, who have developed the tool and who are using it to assist their clients in the AEO certification process. We compare the interview results to identify differences in the expert interpretation of the AEO self-assessment task and in the requirements to obtain AEO certification. To structure the analysis of the expert interpretations, we use conceptual models taken from the CommonKADS methodology [17] and from the literature on risk management. Overlaps and differences between interpretations are mapped, using ontology mapping [18] [12].

The remainder of the paper is organized as follows: Section 2 describes our approach towards a conceptual model of mental model mappings; Section 3 describes our analysis of the case study of AEO self-assessment. The paper ends with a discussion and conclusion of our results.

2 Towards a conceptual model

To identify requirements for an innovative E-government solution that concerns public-private partnerships, such as the AEO certification procedure, we propose Normative Multiagent Systems (NMAS) as a starting point for an analysis. Each stakeholder is viewed as an autonomous agent that can act, perceive its environment, communicate with others and has skills to achieve its goals and tendencies [22]. Although agents are autonomous, their behavior must be restricted by norms. The regulator, which enforces the norms, is also seen as one of the agents and not as a separate entity [2]. This makes sense in our case, because for public-private partnerships, both regulator and businesses have to interpret the legislation to apply it in practice. Figure 1 shows a situation in which two agents 'A' and 'B' must collaborate. To do so, they must interpret norms, and implement them in practice. For each agent we draw two 'thinking balloons': the agent's own interpretation of the norms, and the agent's beliefs about the other agent's interpretation of the norms.

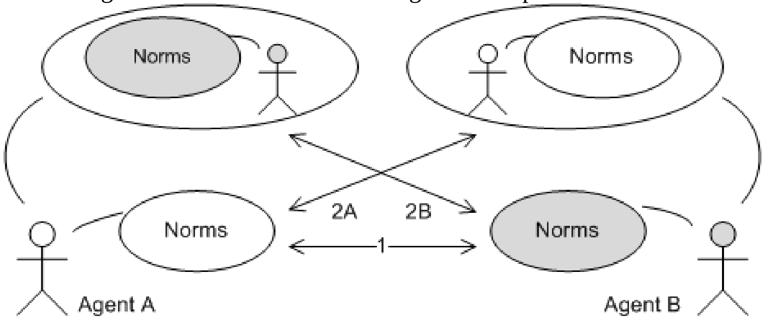

Fig. 1. Agents' beliefs about the norms, and about each other's beliefs of the norms

We suggest that for successful collaboration both agents must have either a shared interpretation of the norms or that their mental models are transparent for the other, so that other agents can adjust their behavior and overcome differences. Uschold and Gruninger [20] also argue that for software agents or IT systems to successfully communicate with each other, they need to be semantically integrated. Successful exchange of information means that agents understand each other and accuracy is guaranteed [20]. This requires that agents must agree on a communication standard or protocol and a common ontology. However in the real world often various ontologies exist about a single topic, so we better speak of semantic heterogeneity than of semantic interoperability [12] .We therefore include a need for transparency in our model. The assumption is that if agents have knowledge about each others' interpretation of the norms, they can predict each others' behavior and task performance, and can adjust their actions accordingly.

To analyze the expected effectiveness of the collaboration we can therefore compare the thinking balloons in two ways (see Figure 1): arrow 1 compares the agent's mental models of the norms, and arrow 2A en 2B compare the mental model with the beliefs the other agent has about the mental model. We also note that the agent's mental model and the belief about the other agent's model can influence each other but this interaction is not addressed in this paper. To assess overlap between the mental models and the beliefs about the mental models we use a technique from software engineering: ontology mapping [18] [12]. Ontology mapping techniques and formalisms are intended to overcome the issue of heterogeneity by identifying the differences and similarities between ontologies. We view the agents in our example as two agents that need to have a (partial) mapping of their ontologies to communicate and collaborate effectively. To promote the merger of ontologies towards semantically interoperable ontologies a first step is to identify the overlapping concepts and key differences. With the differences and commonalities made explicit, the agents become aware about each others mental models, which can in turn help them to more effectively discuss and overcome the differences.

There are various techniques for finding correspondences between semantically related entities of different ontologies. Most matching techniques require the existence of a commonly shared body of knowledge, structure, language or syntax. However in an innovative public private partnership where both the businesses and government have to adapt to their new roles, commonly known responsibilities and ways of interaction do not exist yet. The shared body of knowledge is evolving as best practices are developed, procedures are maturing and lessons are learned based on experiences in the field. Research with a multi agent systems viewpoint does address this issue with the introduction of meaning negotiation or semantic negotiation [3] [6]. These techniques offer a dynamic and flexible form of semantic coordination for situations in which no a priori coordination exists. Bouquet et al. introduce in [3] a method that makes the meaning of nodes in structured semantic models explicit by combining three types of knowledge: lexical, domain and structural knowledge. They combine the knowledge sources to build a new representation of the problem, where the meaning is encoded as a set of logical formulae. Another approach to match ontologies is provided by instance based methods [**7**] [16]. These methods focus on the most active parts of the ontologies and reflect the semantics of the concepts as they are actually being used [16]. Instance-based ontology matching techniques determine the similarity between concepts of different ontologies by examining the extensional information of concepts [**7**]. Various approaches to instance based methods exist: in [**7**] machine learning techniques are used to identify mappings and in [16] a lexical search engine is used to map instances from different ontologies. Concept classification information is exchanged between these mapped instances, to generate an artificial set of common instances shared by concepts from two ontologies, so that simple similarity measures can be applied. The advantages of this method are that it does not depend on the availability of concept labels or a rich ontology structure.

For the matching of mental models of agents in a regulatory setting in which no prior coordination model exist we propose a combination of techniques and different knowledge sources. To construct the mental models in a structured way and to function as a common reference model we propose the use of generic knowledge model templates, from knowledge engineering methods such as CommonKADS [17]. The domain independent nature of such templates provides a good basis for the agent specific models. In line with the CommonKADS method, the agent's models we construct will therefore consist of three knowledge categories: domain knowledge, task knowledge and inference knowledge [17]. Besides that we use legislation and norm frameworks as background domain knowledge to assess the validity of mappings. Then we can determine if concepts relate to the same topic and have a similar or compatible meaning. Furthermore we use instances, implementations of the norms, to derive concepts and mappings. We illustrate the method by a short example of different interpretations of risk assessment, taken from the case study.

The 'Assessment' knowledge model template [17] will function as a starting point to model the risk assessment approaches of a company and the regulator. We can then compare the deviations of the approaches with the original model and since the skeleton is similar we can also compare both risk assessment approaches. To assess the validity of matched concepts we use legislation to determine the meaning. For example the concept *security* can be aimed at preventing theft, taking goods out of the supply chain or preventing smuggling and terrorism, adding things to the supply chain, or a combination of both. Furthermore we use observations in the real world to trace back to which concepts they refer. For example a gate can be seen as an instance of the concept *measure* to prevent intruders from entering a company's premises. While a personal policy can also be seen as a *measure* to avoid the hiring of untrustworthy personnel.

Combining these issues, we come to a three step approach to analyze and compare mental models of agents. Step 1 is to develop generic domain, task and inference models based on knowledge templates from CommonKADS [17]. These generic models are used as a starting point for constructing the agent's specific mental models. Step 2 is to use the generic models to externalize, analyze and compare individual agent's mental model constructs. Step 3 is to build a conceptual model that presents the encountered differences and similarities of the mental models of the agents. This model makes the differences in mental models transparent, which makes it easier to overcome the heterogeneity or to adjust the models accordingly. The following section describes the application of this approach to a case study.

3 Case study: AEO self-assessment of a petrochemical company

We use the approach described in the previous section to analyze a specific case of an AEO self-assessment, which is part of the application procedure for companies to qualify for AEO. The AEO self-assessment is a nice example of collaboration between public and private parties, because a traditionally public task (AEO assessment) is partly delegated to a private party (a company). The private party therefore needs insight in the mental model of the public party (customs authority) to perform the task according to their standards. The customs, on the other hand, are interested in the mental model of the company, because the legislation is new and customs need to learn from best practices of early AEO applicants. The next paragraph provides a short introduction to the AEO legislation and certification procedure.

3.1 AEO legislation and certification

An Authorized Economic Operator (AEO) can be defined as a company that is reliable throughout the EU in the context of its customs related operations [9] [10] [12]. The holder of an AEO certificate will receive several benefits in customs handling within all EU member states that can lead to considerable cost-reductions for businesses. The degree to which a company is granted these facilities depends on the type of certificate: ‘Customs simplifications’, ‘Security and safety’ or ‘Combined’. For non-certified enterprises customs will continue to carry out the traditional supervision. The flow of goods for customs will therefore consist of two parts: goods from AEOs and goods from non-certified companies. Customs can direct their efforts towards non-certified companies to increase the security of international supply chains, while at the same time reducing the administrative burden for AEOs.

To qualify for the AEO status a company must meet a number of criteria, which are described in the community customs code and the AEO guidelines [9].The general customs’ certification practice is that customs officials visit a company which applied for a license, to assess whether the company complies with the legislation and whether a license can be issued. In the AEO certification procedure however, a company must first perform a self-assessment of their compliance to the AEO legislation. The left swim lane in Figure 2 presents the steps that a company has to perform in the self-assessment and the right swim lane shows the activities of the customs in the AEO certification. The first step is that a company collects information relevant for the AEO status, such as business processes, safety procedures, licenses and certificates, IT systems, etc. The next steps are to identify the (potential) risks to which the business is exposed (using the AEO guidelines), to identify the measures that are implemented to mitigate these risks, and to further specify the generic AEO criteria and turn them into internal norms which evaluate the risk mitigation in relation to the line of business. For example, computer components are valuable goods, which are subject to theft. Trading valuable goods requires more security measures, than, say, trading in a mass product like fertilizer. However, some ingredients of fertilizer may be used to assemble explosives, leading to a different set of risks. By evaluating the risk mitigation strategies, a company must determine if the risks are mitigated sufficiently, or if additional measures are needed.Then a company must evaluate the effective implementation of the proposed measures, using the COSO internal control scoring definitions, which are part of the summary of the AEO self-assessment. The scores range from 0 “no control measures in place” until 5 “internal control measures are integrated into the business processes and continuously evaluated”. After that the company either submits the AEO application or implements (additional) measures.

Once the customs receive the AEO application, they assess whether it is a valid application according to entry conditions. Next, they determine the type of visit, based on the AEO application and on historical data about customs and tax compliance. A visit is needed to check whether the self-assessment is performed correctly and whether the company identified all the risks and has taken all appropriate measures.

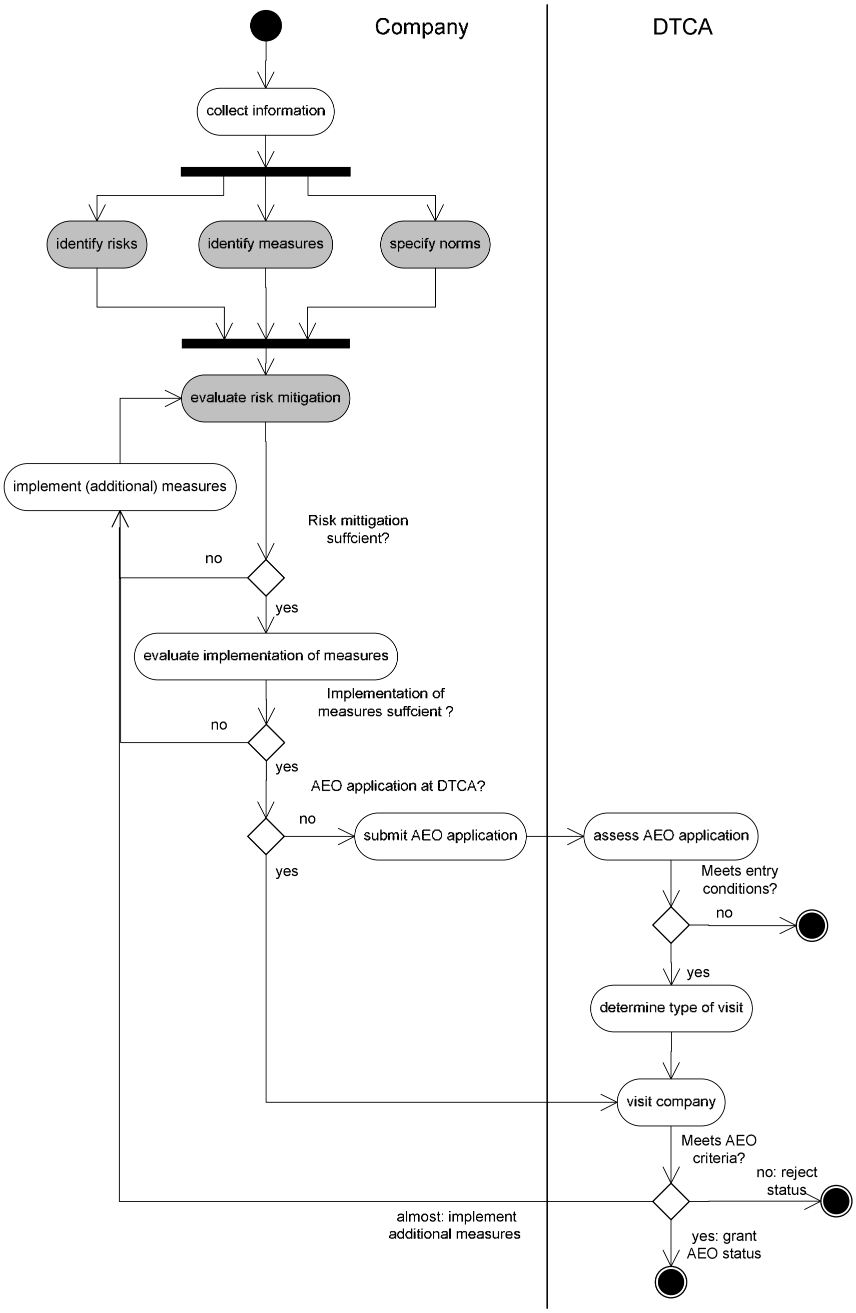

Fig. 2. Activity diagram for the AEO certification procedure. Activities in grey are supported by the AEO Digiscan.

Based on the visit, customs determine whether the AEO certificate is granted or not or that first additional measures need to be implemented. In that case, customs will visit the company a second time, to check if the additional measures are implemented.

Ideally, a company would perform the self-assessment like customs would, when they are ‘auditing’ a company for AEO compliance. The customs authority could then rely on the findings of the company and minimize their own visit. However, from interviews with DTCA officials we learned that companies often find it difficult to perform an AEO self-assessment. Consultancy firms therefore offer services and tools to assist companies. One of these firms is Deloitte and their tool is called the AEO Digiscan. The steps in the process which are supported by the Digiscan are colored dark in Figure 2. The next section describes the Deloitte AEO Digiscan in more detail.

3.2 AEO Digiscan

To support companies in performing the AEO self-assessment Deloitte’s Tax Advise unit developed the AEO Digiscan. The AEO Digiscan is an online tool that works as a classic expert system. It contains rules, which represent the AEO guidelines and the sections in the questionnaire are organized accordingly. Various experts of Deloitte such as tax advisors, security specialists, IT specialists and auditors contributed to the development of the AEO Digiscan, by specifying the guidelines, and turning them into clear questions. The questions that a company has to answer depend on the company’s role in the supply chain and on answers to earlier questions. Scores are expressed on a 5 point scale ranging from red (1) till green (5). For example, red (1) means “Potential risk can be considered high”, orange (3) means “Potential risk could neither be considered low nor high” and green (5) means “Potential risk could be considered low and acceptable”. The score of each section is based on the lowest score in the section and cannot be altered after a section is completed. After answering the questions, experts of Deloitte check the AEO Digiscan results. They have the possibility to adjust the scoring if they think a company has overestimated or underestimated its record. After that the risk based score of the AEO Digiscan is automatically translated into the COSO based scoring used by DTCA, and the AEO summary is filled out. Deloitte sends the AEO Digiscan report and the AEO summary with feedback to the company. The company can then decide to send the AEO application to DTCA.

The added value of the tool is that it provides a structured approach to AEO self-assessment. It assists companies in interpreting and applying the AEO guidelines. Furthermore, it provides companies with an indication of their position with respect to achieving the AEO status, and points out their strengths and weaknesses.

When a company uses the AEO Digiscan to perform a self-assessment, we can view this as another delegation of the self-assessment task, namely to Deloitte‘s AEO Digiscan. To assure that the self-assessment task is performed as intended by DTCA, it is therefore important to also assess the overlap between the mental models of Deloitte and DTCA, besides the regular mapping between company and DTCA. In this paper we will focus on the mapping between Deloitte and DTCA. The next section describes our analysis of the AEO self-assessment task.

3.3 Case analysis

This section presents our analysis of the differences and overlap that exist between the approaches of AEO self-assessment of DTCA and Deloitte. We perform our analysis according to the steps described in Section 2. For the data collection we used the following methods: document analysis and semi-structured interviews [24]. We studied internal and public documents from both DTCA and Deloitte that describe their vision and approach on AEO certification and self-assessment. To gain insight in the expert interpretation of the AEO self-assessment, we conducted 5 interviews with both DTCA and Deloitte, held one meeting were we invited both parties simultaneously, joined DTCA auditors on their first visit to a petrochemical company and held a first feedback session for both DTCA and Deloitte to present our initial research results. To elicit detailed expert knowledge, we showed the experts the AEO application of a petrochemical company "PCC", which had used the Deloitte AEO Digiscan, and asked them how they would have assessed this company (if there would have been no AEO self-assessment) and if they could point out points of interest. We also asked them some questions about the AEO certification and self-assessment in general. In total we have spoken with 10 persons from DTCA and 5 from Deloitte. The duration of the interviews varied from 2- 4 hours. Except for the visit, the meeting and a first interview with Deloitte, we tape-recorded all interviews with the participants' prior agreement. Minutes were made of meetings.

3.3.2 Domain, task and inference model

To analyze the interview results, we use an adapted version of the knowledge model templates for the assessment task of the CommonKADS methodology [17].To save space; we do not show a task model in this paper. Figure 3 represents the domain schema for AEO certification. The purpose of this model is to specify key concepts and indicate how they are related. The implementation of these relationships is then further worked out in the inference structure, which we present in Figure 4.

First we have to identify the domain. A company is eligible for an AEO certificate, when it conforms to four criteria: (1) an appropriate record of compliance with customs regulations, (2) sufficient internal control measures regarding trading and logistics, to allow for customs auditing, (3) conformance with certain solvability criteria, and (4) appropriate security measures to safeguard the supply chain. In the interpretation of DTCA, the AEO self-assessment is essentially a statement in which the company declares to be `in control' of its supply chain. Under the current interpretation of DTCA, this means that the company must have performed a risk assessment to identify key risks regarding security in the supply chain, must have taken appropriate control measures to mitigate the risks, and must have evidence that these measures have been operationally effective. So a conceptual model of risk management seems a good starting point for domain analysis. Risk management is the activity – performed by management – of continuously assessing risks, defining and implementing control measures to mitigate risks and evaluating and improving the results. A well known best practice for IT risk management has been proposed by NIST. They define a risk as a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization [19]. Similar definitions are found in other literature on risk management.

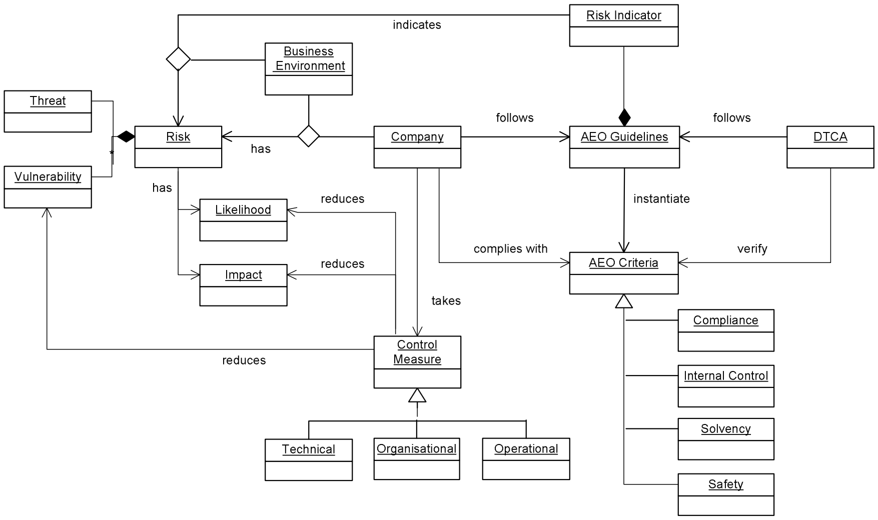

Fig. 3. Domain schema for AEO certification

The left of Figure 3 shows general risk assessment concepts. A risk assessment identifies the threats facing a company given its line of business and its environment. The vulnerability of a company to threats depends on its current control measures. Control measures either reduce the likelihood, by dealing with vulnerabilities (preventative controls), or reduce the impact (detective and corrective controls). Consider for example the risk of smuggling: someone secretly places an additional item in a container. This vulnerability can be reduced by limiting physical access to all premises where containers are loaded and unloaded, to those employees who need to have access because of their job. In general, there are three kinds of control measures: technical controls (e.g. authentication by RFID badge), organizational controls (e.g. access control based on real needs) and operational controls (e.g. reconciliation of shipping order against inventory). On the right we show the AEO criteria and the AEO guidelines. The guidelines do not act like norms, as one might expect. They are merely high-level attention points, which – given a business environment – indicate the main risks for the company. It is the responsibility of the company to set their own internal norms, depending on the actual risks encountered.

Figure 4 depicts the inference structure for AEO self-assessment. It is the generic assessment model, taken from [17]. The input for the inference is the case, a description of the company that applies for AEO status. First, a company must abstract case data that corresponds with the data used in the norms. For the AEO self-assessment this means that a company has to identify all the potential risks, the measures that mitigate these risks, and the implementation of the measures, related to its business activities and role in the supply chain. A company must then specify which (sub) sections addressed in the AEO guidelines are applicable to the company's specific situation and need to be evaluated and reported in the AEO summary. From this set of (sub) sections a company selects a single

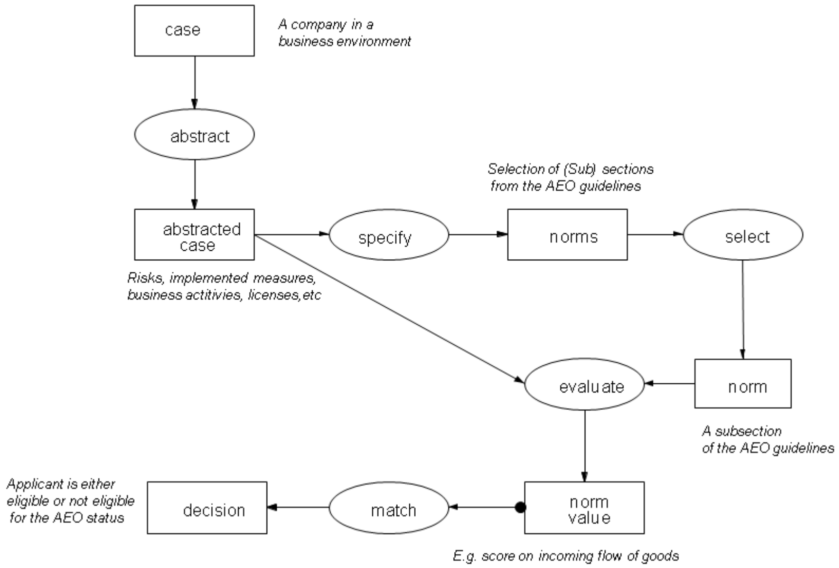
case
A company in a business environment
abstract
Selection of (Sub) sections from the AEO guidelines
abstracted case
specify
norms
select
Risks, implemented measures, business actitivies, licenses,etc
evaluate
norm
A subsection of the AEO guidelines
Applicant is either eligible or not eligible for the AEO status
decision
match
norm value
E.g. score on incoming flow of goods

Fig. 4. Inference structure of the assessment task (Schreiber et al 2000)

subsection for evaluation. For each subsection a company determines if the risk mitigation is sufficient and evaluates the implementation of the measures. The output value is an integer (0-5) indicating the implementation level of the measures, which a company reports in the AEO summary. The match function checks whether the scores on the self-assessment summary lead to a decision if a company is AEO compliant or not. The match function only stops prematurely in case of (clear) incompliance. A company is only AEO compliant when it scores well on all the (sub) sections that are applicable.

3.3.3 Constructing and comparing mental models

Now we present the interview findings, organized according to the inference model of the previous paragraph.

Abstract: The ‘abstraction’ inference is a complex step. Essentially it is a form of classification, which abstracts over individual differences. According to DTCA, to properly evaluate the mitigation of risks, they have to be evaluated in context. This includes the business activities, company role in the supply chain, organizational structure, location, etc. Case data about all these aspects and their interaction, needs to be combined in an abstract classification. There is no structured approach available to classify the type of company; DTCA only advises the companies to use the AEO guidelines to identify risks. Classification in the AEO Digiscan is a lot simpler. It only looks at risks and measures related to the company’s role in the supply chain.

Specify: The AEO guidelines contain a table that indicates which of the (sub) sections of the guidelines are applicable, based on the company’s role in the supply chain. A company can also decide to leave out or include certain subsections based on its specific business activities, e.g. when a company is both a manufacturer and an exporter. The AEO Digiscan makes use of this table and automatically presents only the questions related to the company’s role in the supply chain. Experts of Deloitte made the AEO guidelines more specific, specifying questions that are easy to understand. Based on previous answers the tool selects the next question. However, DTCA officials believe that the AEO guidelines have been implemented too literally and that it does not take the business environment into account. For example, the AEO Digiscan contains very general questions about IT, such as: “Which operation system is used in your company?” to which PCC answered: “Windows”. However, no questions are asked about the IT systems used in the manufacturing process. PCC is partially a manufacturer, so a risk to its key business processes is a threat to a secure supply chain. DTCA officials also realize the limitations of a tool like this, and wonder how an electronic questionnaire can ever be complete, if it has to take all these specific characteristics into account.

Select: The DTCA approach requires the manual selection of subsections of the guidelines. The AEO Digiscan automatically selects and presents a question, on the basis of answers to the previous questions.

Evaluate: The evaluation step requires companies to first perform a risk assessment, in which the adequacy of the risk mitigation is assessed relative to the business context, and second to evaluate the implementation of these measures. DTCA does not provide a step by step approach to do the evaluation. A company must itself determine its COSO level on all applicable subsections in the AEO summary. The AEO Digiscan focuses on risk assessment and identifies potential risks and the measures that are in place. After a section is completed, the tool automatically calculates the potential risk level for the subsections and the whole section. According to a DTCA official: *“A tool should not let people answer questions without knowing why they answer them. It should first give a good overview of the purpose of the specific questions”*. If people do not understand the purpose of a question, they can misinterpret the question and give the wrong answer. Furthermore, hiding the ‘abstraction’ inference from the user turns the self-assessment into a checklist that can be filled out without creating awareness on internal control or safety measures.

Match: After the AEO Digiscan is completed, it provides for each subsection an indication of the company’s position with respect to achieving the AEO status. To prevent fraud, DTCA does not tell companies what a sufficient score is to achieve the AEO status. The companies receive the first feedback on their scores during the customs visit.

In general we find that the approach offered by the AEO Digiscan is more structured and requires less expertise on AEO legislation, than the general approach that is proposed by DTCA. However, the scope of the AEO Digiscan is limited; it focuses on risk assessment (identifying risks and measures) while DTCA’s approach focuses on risk management, including implementation of measures. Although the tool is limited, it provides for a consistent assessment process. DTCA officials asked for insight in the scoring calculation mechanism of the AEO Digiscan. Deloitte would have liked more insight in DTCA’s requirements and into their evaluation approach. Furthermore we noticed that DTCA pays a lot of attention to the reliability of the self-assessment and to the way it was performed, while Deloitte’s focus is more on specifying the AEO legislation and AEO guidelines.

3.3.4 A conceptual model of scoring

We will further zoom in on the differences in the scoring model, which is an important issue according to both parties. The grey concepts in Figure 5 are only covered by the DTCA approach; the white concepts are part of both approaches. We observe that the AEO Digiscan covers only part of the DTCA approach. The AEO Digiscan focuses on risk assessment, whereas the self-assessment, as it is interpreted by customs, involves risk management, which also stresses the need for additional measures and evaluation. This is in line with the views that DTCA and Deloitte have on AEO certification. DTCA sees the AEO self-assessment as a means to judge the quality of companies' internal control system, and to create awareness of potential risks. In contrast, Deloitte efficiently provides companies with an indication of their readiness to achieve AEO status. The Deloitte approach is therefore more aimed at compliance with AEO legislation, whereas the DTCA approach aims at companies being 'in control' of their internal procedures regarding safety and security. The AEO Digiscan tool supports the compliance assessment through a bottom up approach: answer specific questions to arrive at an overall score. DTCA's approach works top down: to be in control, what measures does a company need to have implemented?

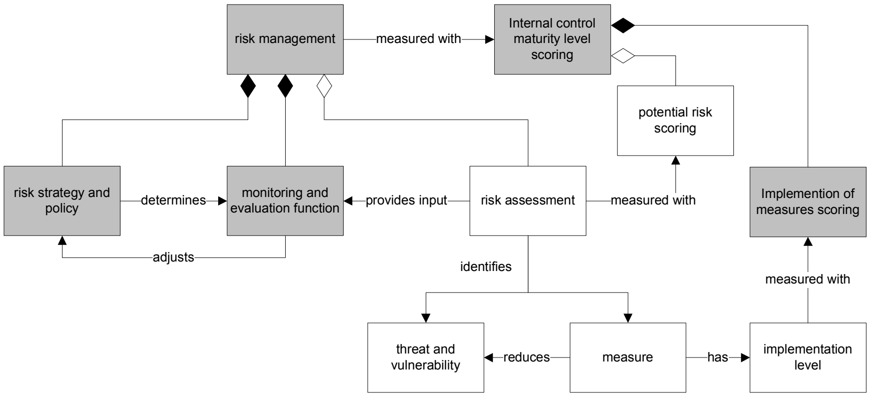

Fig. 5. Model of differences (dark) and overlap between DTCA and Deloitte

The different scoring models are in line with these different views on self-assessment. DTCA uses the COSO scoring, which measures the implementation of control measures and Deloitte uses a risk-based scoring. By making the differences in the scoring models explicit we pointed out to DTCA and Deloitte that Deloitte's risk-based approach is a step within DTCA's approach rather than a complete different approach. Aligning the approaches is therefore easier to achieve than it looked at face value. The interpretation of all these aspects needs to be addressed in the early requirements phase as they can lead to various system requirements. Should the AEO Digiscan support DTCA's risk management approach or should Deloitte focus on risk assessment only, and embed its tool in DTCA's approach? Should we use a risk based scoring method and do we need to include the implementation of the measures? This greatly influences the kind of tool that is developed and the role the tool will fulfill within the task of "self-assessment".

4. Discussion and conclusions

4.1 Regarding the research method

This paper reports on initial exploratory research. Interviewing proved to be a good research technique to gain insight into the AEO self-assessment approach of both Deloitte and DTCA, as our interviews uncovered some very interesting issues. However the number of interviews was limited, especially for Deloitte, where we only interviewed 5 people. Furthermore, our interviews were semi-structured and therefore not all topics were addressed consistently in all interviews. We therefore want to validate these results with a second round of interviews, using a more controlled set up. Another point is that we compared the expert knowledge embedded in a tool with real expert knowledge. The embedded knowledge was more explicit and therefore easier to compare, but it is already a selection of the expert knowledge of the Deloitte experts. On the other hand the AEO Digiscan gave us a good view on which part of the expert knowledge is easy to externalize and to imbed in a tool. Besides that we ourselves made the task and domain models based on the interview findings. It can therefore be argued that another interpretation was added to the mental models of the experts. In fact, we also compared original models used by the experts. However, since the Deloitte approach is based on the DTCA approach, comparing the models did not provide any results. The differences we encountered in the interviews were more concerned with the interpretation of the concepts by the experts. The expert interpretation of the domain (see Figure 3) was shared among the experts of both parties.

4.2 Regarding the mapping of mental models

Based on our interview findings we can conclude that by and large, the interpretations of the task and domain model for AEO self-assessment by experts from Deloitte and from DTCA overlap. Both make use of risk analysis methods and are based on the AEO guidelines, and therefore use similar attention points. However, important aspects of the self-assessment are interpreted differently. Regarding the task, there is disagreement about the scope of the self-assessment: does it only contain risk assessment (AEO Digiscan) or is it concerned with risk management, which also includes the implementation and constant evaluation of control measures (DTCA)? These task differences also show up in the domain analysis and the inference scheme. In particular, they lead to different scoring models: a risk-based model for AEO Digiscan, and COSO-based maturity levels for DTCA. There are also diverging ideas about the role of ‘understanding the business’ when assessing risks and controls. DTCA experts stress that control measures must be understood in context. For example, the strength of password protection must be interpreted relative to the business environment and IT infrastructure. Deloitte experts, on the other hand, have tried to further specify and instantiate the generic AEO guidelines into specific questions. Moreover, an initial classification of the company will automatically select only the relevant questions. But despite such customization, the tool does not allow for any company specific considerations. As a benefit, this generic nature of the AEO Digiscan improves the transparency and reliability of the assessment procedure. Our methodology does not require completely shared mental models. Differences of opinion or mental model are fine, as long as parties know the differences, and know how to adjust their behavior accordingly (Figure 1). For requirements engineering, this means that mental models about other stakeholders have to be modeled explicitly as this helps them to realize what their respective positions are, and act accordingly. From the case study it even became clear that making differences explicit is often the first step towards solving the differences. Our analysis made the Deloitte experts aware what the differences between both approaches exactly are and that the difference concerned a scope problem rather than a complete mismatch. This insight has led to Deloitte taking action to adapt their tool and risk-based scoring model, to increase the overlap between their and DTCA's approach. In contrast with some of the empirical literature on shared mental models [4][14]we have attempted to make mappings of the actual differences and overlaps. To this end, we have used template models from CommonKADS [17]. Regarding these templates we can conclude that they have been instrumental in bringing out and explaining some key differences. For example, the difference between a case description and an abstracted case (Figure 4) turns out to reflect the effects of the loss of information in the AEO summary. Also the activities of specifying and selecting norms (Figure 4) explain important differences of opinion.

4.3 Regarding the AEO Digiscan decision support tool

Charting the differences between mental models of stakeholders is an important element of developing a complex decision support system, because it helps to identify differences in expected functionality, and in the way the system is expected to be used. Differences in task and domain models will lead to different system requirements, consider for example the scoring models. Therefore such mental model mapping should be part of early requirements engineering [5][23]. Note that some expectations may be too complex. It is easier to design and implement an expert system about compliance (rule-based), than about risk assessment in context (principle-based). A less ambitious system, with a task that naturally aligns with one or more sub-tasks of the task model, may be easier to get accepted, than an overly ambitious system which will disappoint some stakeholders.

Mapping overlaps and differences is especially important in a regulatory context. The regulator is leading. But also the regulator needs material on which to base its benchmarking. It cannot develop norms by itself, but has to use 'best practices' of companies. The experience of using a decision support tool has proved very useful in this respect, as the tool has forced experts to be specific about their intentions.

For future research we would like to narrow the focus of the research and try to make a more elaborate analysis of the differences. We are currently arranging more interviews with IT auditors from both Deloitte and DTCA, to zoom in on the IT aspects of AEO certification.

Acknowledgments. This research is part of the integrated project ITIADE which is funded by the 6th Framework IST Programme of the European Commission. We are grateful for the open discussions with representatives of DTCA, Deloitte and PCC.

References

1. Baida, Z., Rukanova,B., Liu,J. & Tan,Y. (2008)Preserving Control in Trade Procedure Redesign - The Beer Living Lab,Electronic Markets, The International Journal, Vol. 18, No. 1, pages53-64
2. Boella, G. and van der Torre, L. (2007). Norm negotiation in multiagent systems. International Journal of Cooperative Information 16(2), pp. 97-122.
3. Bouquet, P. Serafini, L. and Zanobini, S. Semantic Coordination: A New Approach and an Application, Proc. ISWC2003, Springer, LNCS 2870, 130-145, 2003.
4. Cannon-Bowers, J.A. & Salas, E. (2001) Reflections on Shared Cognition. Journal of Organizational Behavior, Vol. 22, No. 2, pp. 195-202
5. Castro, J., Kolp, M., and Mylopoulos, M. (2002) Towards requirements-driven information systems engineering: The Tropos project, Information Systems (27), pp. 365–389.
6. Van Diggelen, J., Beun, R. , Dignum,F., van Eijk, R., Meyer, J. (2007) Ontology Negotiation: Goals, Requirements and Implementation. International Journal of Agent-Oriented Software Engineering 1(1):63–90.
7. Doan, A.H., Madhavan, J., Domingos, P., Halevy, A. (2002) Learning to map between ontologies on the semantic web. In: Proceedings of the 11th international conference on World Wide Web, pp. 662–673
8. van Engers, T.M., Kordelaar, P.J.M., den Hartog, J., Glassée, E., (2000) POWER: Programme for an Ontology based Working Environment for modeling and use of Regulations and legislation. Proceedings 11th workshop on Database and Expert Systems Applications (IEEE) Greenwich London, pp. 327-334.
9. European Commission (2007) AEO Guidelines, TAXUD/2006/1450.
10. European Commission (2006) The AEO Compact model, TAXUD/2006/1452.
11. Euzenat, J., Shvaiko, P. Ontology Matching. Springer, Heidelberg (2007)
12. Kalfoglou, Y. & Schorlemmer,M.(2004) Formal support for representing and automating semantic interoperability. ESWS 2004, pp. 45–60
13. Kalfoglou, Y. & Schorlemmer, M. (2003) Ontology mapping: The state of the art. The Knowledge Engineering Review, Vol. 18:1, 1–31
14. Mohammed, S. & Dumville, B. C. (2001). Team Mental Models in a Team Knowledge Framework: Expanding Theory and Measurement Across Disciplinary Boundaries. Journal of Organizational Behavior, 22(March): 89-106.
15. OECD (2005). E-Government for Better Government, Organization for Economic Co-operation and Development.
16. Schopman, B.A. C. Wang, S. and Schlobach, S.(2002) Deriving Concept Mappings through Instance Mappings, In John Domingue and Chutiporn Anutariya, editors, ASWC, volume 5367 of Lecture Notes in Computer Science, pages 122-136
17. Schreiber, G., Akkermans, H., Anjewierden, A. , de Hoog, R., Shadbolt, N., Van de Velde, W. and Wielinga, B. (2000) Knowledge engineering and management, MIT Press.
18. Sowa, J. (2000) Knowledge Representation: Logical, Philosophical, and Computational Foundations. MIT Press.

19. Stoneburger, G., Goguen, A. and Feringa, A. (2005) Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30
20. Uschold, M. & Michael Gruninger, M. (2004) Creating Semantically Integrated Communities on the World Wide Web. Invited Talk Semantic Web Workshop
21. Wimmer, M.A. (2002) A European perspective towards online one-stop government: the eGOV project. Electronic Commerce Research and Applications 1(1): 92-103
22. Wooldridge, M. (2002) An Introduction to Multiagent Systems, John Wiley & Sons (Chichester, England).
23. Yu, E.K.S. (1997) Towards Modelling and Reasoning Support for Early-Phase Requirements Engineering, in: Proceedings of the Third IEEE International Symposium on Requirements engineering, pp. 226-235.
24. Yin, R. K. (2003) Case study research: Design and methods. Sage Publications Inc.