TrustCoM

Deliverable

17

Appendix A

Method and language for legal risk management

WP9 Legal Issues

Fredrik Vraalsen, SINTEF
Tobias Mahler, NRCCL

9 February 2006

Final Version

TrustCoM

A trust and Contract Management framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations

SIXTH FRAMEWORK PROGRAMME

PRIORITY IST-2002-2.3.1.9

Prepared for the European Commission under FP6 Contract No. 01945 as a deliverable form

Table of Content

1 Introduction ... 3
1.1 Risk management method ... 4
1.2 Graphical language ... 5
2 Evaluation of method and language ... 7
2.1 Method ... 7
2.1.1 Guidewords ... 8
2.2 Graphical language ... 8
3 Method for model-based legal risk management focusing on trust and security issues in VOs ... 10
3.1 Introduction meeting ... 11
3.1.1 Client presents system or organisation ... 12
3.1.2 Characterise focus and scope of the analysis ... 13
3.1.3 Plan the analysis ... 13
3.2 High-level analysis ... 14
3.2.1 Risk analysts present target of analysis ... 14
3.2.2 Identify assets ... 16
3.2.3 High-level risk analysis ... 16
3.3 Approval meeting ... 17
3.3.1 Target of analysis documentation ... 17
3.3.2 Asset values ... 18
3.3.3 Risk evaluation criteria ... 18
3.4 Risk identification ... 19
3.4.1 Structured brainstorming ... 19
3.5 Risk estimation and evaluation ... 21
3.5.1 Estimate risk level ... 21
3.5.2 Evaluate risks ... 22
3.6 Risk treatment ... 22
3.6.1 Identify treatments ... 22
3.6.2 Evaluate treatments ... 23
3.7 Finalisation meeting ... 23
4 Legal checklist ... 24
4.1 EN or VO Internal Relations ... 25
4.2 The Relation to the End-User ... 26
5 Graphical language for legal risk management ... 28
5.1 Modelling legal aspects using UML ... 28
5.2 Extensions to the CORAS language ... 31

1 Introduction

Virtual Organisations' dependency on information and communication technology for performing their daily work leads to a number of risks related to security, trust and legal issues. Some areas where VOs face risks is the protection of intellectual property (IP) and confidential information, access rights management, and data protection. The risks are further exacerbated by the international nature of many VOs, as well as their dynamic nature where participants can join and leave the VO at any point during its lifetime. These areas have been the focus of the legal risk analyses performed of the TrustCoM test-bed scenarios and presented in WP9 deliverable D15 as well as appendix B of this report.

There is no general international legal framework for the establishment and operation of virtual organisations, and legal issues in relation to VOs are still a topic for research. A recently published strategic roadmap for advanced virtual organisations points out that the analysis of legal risks arising in operating VOs and the development of legal strategies to overcome them is an important research task in order to support collaborative networked organisations[1]. Others have addressed more general project risk management[2,3]. Such strategies should focus both on the contracts that need to be put into place and on the technology that may be utilized in order to facilitate and support the collaboration. The collaboration of different experts, like computer scientists and lawyers, is necessary when analysing what may go wrong in a co-operation[4,5].

To reduce the risks involved with establishing, joining and operating a VO, an approach is needed for analysing and managing legal risks which takes into account both technical and non-technical aspects. One of the goals of TrustCoM WP9 has been to develop methods and languages to facilitate legal risk analysis. These have been based on the existing CORAS model-based security risk analysis method and graphical threat modelling language. The work in WP9 has focused on application and adaptation of the CORAS language and method to the integrated

[1] Camarinha-Matos, L., Afsarmanesh, H., Löh, H., Sturm, F., Ollus, M. (2004). *A strategic roadmap for advanced virtual organizations*. In collaborative networked oganizations: a research agenda for emerging business models. Camarinha-Matos, L., Afsarmanesh, H. (eds.). New York, USA: Springer.

[2] Baccarini, D., Archer, R. (2001). *The risk ranking of projects: a methodology.* International Journal of Project Management 19, pp. 139-145.

[3] Raz, T., Michael E. (1999). Use and benefits of tools for project risk management. International Journal of Project Management 19, pp. 9-17.

[4] Heymann, T. *Outsourcing in Deutschland – eine Bestandsaufnahme zur Vertragsgestaltung. Die Grundtypen des Outourcing und ihre Konsequenzen für die Vertragsgestaltung.* Computer und Recht (2005) 10, p. 706-710.

[5] Müller-Hengstenberg, C. D. (2005). *Der Vertrag als Mittel des Risikomanagements. Ein Plädoyer für die dynamische Projektbegleitung im Vertrag.* Computer und Recht (2005) 5, p. 385-392.

analysis of security, trust and legal issues[6,7,8], as well as continuous improvements of the language based on experiences from use and empirical investigations. Some of the experiences and feedback are summarised in section 2 below.

1.1 Risk management method

The CORAS risk management method is based on the AS/NZS 4360 standard for risk management[9] and integrates aspects from different risk analysis techniques with state-of-the-art system modelling methods based on UML 2.0 (OMG, 2005a), the de facto standard modelling language for information systems.. *Risk management* is the sum of the culture, processes and structures that are directed towards effective management of potential opportunities and adverse effects. The *risk management process* consists of systematic application of management policies, procedures and practice to the tasks of establishing the context and identifying, analysing, evaluating, treating, monitoring and communicating risks. Risk management thus covers the entire lifecycle of the system or organisation, and may include several risk analyses with different focus areas and abstraction levels as the system or organisation and its surroundings evolve over time. The risk analysis process is typically organised as a set of meetings, as summarised in Figure 1 below.

A number of improvements have been made to the method description, and reusable elements have been created in the form of checklists for legal risks and treatments. The updated risk analysis process is described in more detail in section 3 below, while the checklists are presented in section 4.

[6] Brændeland, G., Stølen, K. (2004). *Using risk analysis to assess user trust – A net-bank scenario.* In Proceedings of the 2nd International Conference on Trust Management (iTrust '04). Oxford, UK. Springer LNCS 2995.

[7] Vraalsen, F., Lund, M. S., Mahler, T., Parent, X., Stølen, K. (2005a). *Specifying Legal Risk Scenarios Using the CORAS Threat Modelling Language – Experiences and the Way Forward.* In Proceedings of the 3rd International Conference on Trust Management (iTrust '05). Paris, France: Springer LNCS 3477.

[8] Mahler, T., Vraalsen, F. (2005). *Legal Risk Analysis with Respect to IPR in a Collaborative Engineering Virtual Organization*. In Proceedings of the 6th IFIP Working Conference on Virtual Enterprises (PRO-VE'05). Valencia, Spain: Springer.

[9] AS/NZS. (2004). *Risk Management*. AS/NZS 4360:2004. Australia. Standards Australia.

Meeting 1: Introduction
- Client present the system or organisation they wish to analyse
- Characterise the focus and scope for the analysis, including legal context
- Set up analysis plan

Meeting 2: High-level analysis
- Risk analysts present their understanding of the target of analysis
- Identify assets
- Establish initial threats and vulnerabilities

Meeting 3: Approval
- Target of analysis documentation
- Assign value to assets
- Identify risk evaluation criteria

Meeting 4: Risk identification
- Identify risks through structured brainstorming

Meeting 5: Risk estimation and evaluation
- Estimate likelihood and consequence of risks
- Evaluate risks with respect to risk evaluation criteria

Meeting 6: Risk treatment
- Identify and evaluate treatments

Meeting 7: Finalisation meeting (if necessary)
- Present results and get any missing input

Figure 1 Risk analysis meetings

1.2 Graphical language

Risk analysis requires a clear understanding of the system or organisation to be analysed. This can only be achieved through the involvement of stakeholders and other interested parties with different backgrounds and knowledge about the system or organisation being analysed, e.g. decision makers, security experts, legal experts, system owners, developers and users. These participants are involved in the identification and evaluation of risks and treatments through structured brainstorming sessions.

The effectiveness of such sessions depends on the extent to which the participants are able to communicate with and understand each other. The CORAS graphical language for threat modelling[10] has been designed to mitigate this problem within the security domain. The graphical language is an extension of the UML 2.0 specification language. It is defined as a UML profile[11], and has recently become

[10] den Braber, F., Lund, M.S., Stølen, K., Vraalsen, F. (2005). *Integrating security in the development process with UML.* Encyclopedia of Information Science and Technology. USA: Information Resources Management Association.

[11] Lund, M.S., Hogganvik, I., Seehusen, F., Stølen, K. (2003). *UML profile for security assessment.* Technical Report STF40 A03066. SINTEF Telecom and informatics.

part of an OMG standard[12]. The language covers notions like asset, threat, risk and treatment, and supports communication among participants with different backgrounds through the definition of easy-to-understand symbols associated with the modelling elements of the language. A recent study has shown that the graphical symbols allow the participants to understand and read the diagrams more quickly[13].

Figure 2 shows the main elements of a risk analysis and gives examples of the symbols used by the graphical language. The *target* is the system or organisation, or parts thereof, which is the focus of the analysis. *Assets* are the parts or features of the target which have value to the client of the analysis, such as physical objects, know-how, services, software and hardware, and so on. A *vulnerability* is a weakness of the system or organisation. A *threat* may exploit a vulnerability and cause an *unwanted incident*, an event which reduces the value of one or more of the assets. A *risk* is an unwanted incident along with its estimated likelihood and consequence values. *Treatments* represent various options for reducing risk.

Facilities have been added to the graphical language as well as to UML itself to enable modelling of legal risks and treatments The languages are described in section 5 below.

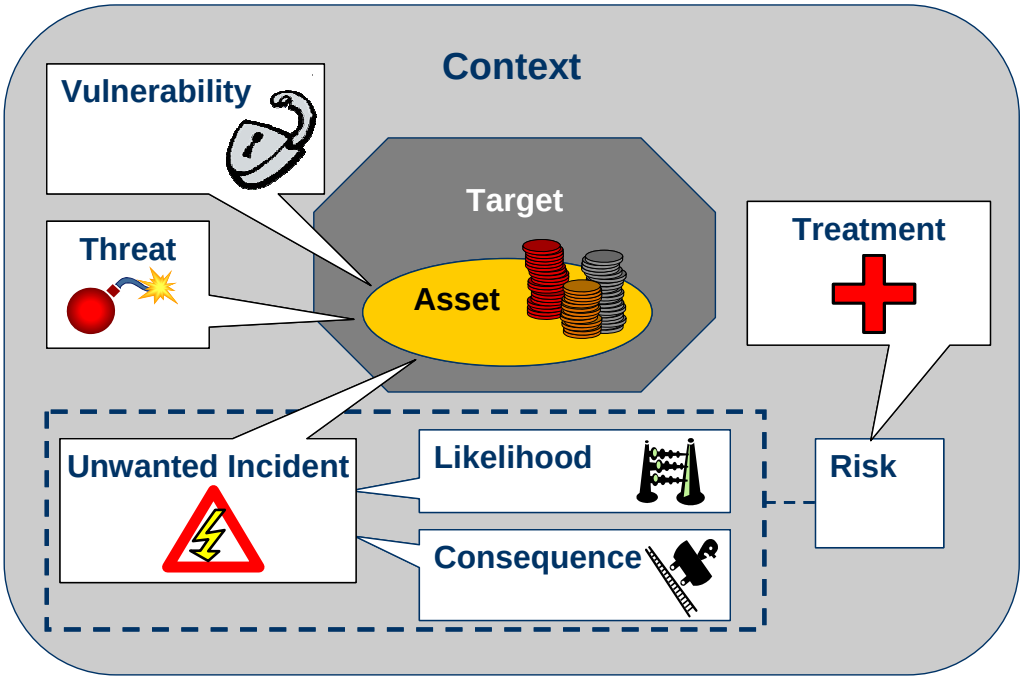

Figure 2 Elements of a risk analysis

[12] OMG. (2005b). *UML Profile for Modeling Quality of Service and Fault Tolerance Characteristics and Mechanisms, Available Specification*. OMG Document: ptc/2005-05-02. Object Management Group.

[13] Hogganvik, I., Stølen, K. (2005). *On the Comprehension of Security Risk Scenarios*. In Proceedings of the 13th International Workshop on Program Comprehension (IWPC 2005). St. Louis, USA: IEEE Computer Society.

2 Evaluation of method and language

As mentioned above, one of the goals of TrustCoM WP9 has been to develop methods and languages to facilitate legal risk analysis. These have been based on the existing CORAS model-based risk analysis method and graphical threat modelling language. A number of risk analyses have been performed of various legal aspects of the TrustCoM scenarios using the CORAS approach. During these analyses, we have evaluated the usefulness of the various parts of the method and language and the adaptations which have been made along the way. The evaluation is based both on our experiences from performing and leading the risk analyses as well as feedback from the other participants of the analyses. These evaluations have resulted in a number of improvements to the method and language to better suit the needs of a legal risk analysis, as well as more general enhancements. The updated method and language are described in more detail in the following sections. Some of the feedback and experiences are presented below.

2.1 Method

- The risk analysis method, in particular the use of structured brainstorming, has proven very suitable for identification of risks and treatments, also in the legal domain.
- The risk analysis helped clarify a number of questions and issues in the scenario.
- The risk analysis steps seem reasonable for businesses – ”they would perform these activities.” In particular, a cost/benefit analysis of the identified treatments would be crucial. The risk analyses performed in TrustCoM have not focused on this aspect of the risk analysis process, but this clearly warrants more attention.
- Fault Tree Analysis was attempted in order to determine the frequency of the identified risks in one of the scenarios. This did not work very well, mainly because of the lack of any real historical information about the behaviour of the system. However, this is useful for structuring incidents and seeing dependencies between them, e.g. which events need to happen for an incident to occur. This has led to the inclusion of facilities for modelling more complex relationships (AND, OR) in the graphical language, as shown in section 5.
- A traditional risk analysis of security or safety tends to focus on the protection of the existing assets. However, when for example drafting a contract, we need to also take into account the business goals and opportunities of the collaboration. A legal risk analysis may thus need to also include goals and opportunities in the analysis rather than just protection of assets.

- Identifying the most important assets can be quite hard. In particular, goals or opportunities, as well as more abstract assets such as reputation, can be hard to define and assign value. Better guidelines are needed in this area.
- Prioritisation of assets is perhaps more important than assigning concrete values – the goal is to identify what the client of the analysis is most concerned about. The same goes for determining risk value: the main point is being able to select which risks need treatment, not necessarily to assign accurate values for likelihood and consequence.
- It is difficult to identify all the (legal) bad things that can happen in a business collaboration. The contract drafted as the result of a legal risk analysis should protect against known as well as unknown risks, e.g. by making the clauses as broad as possible.

2.1.1 Guidewords

The use of guidewords is a technique to structure the brainstorming sessions and to help the risk analysts ask the right questions. The guidewords should be used as a catalyst for discussion.

- The participants thought the use of guidewords would be useful when speaking with the client, helping to identify additional risks which might otherwise have been missed.
- The best way to use the guidewords seems to be to keep the graphical model on screen and then use the guidewords to ask questions, initiating discussion and associations around the threats and assets currently in focus.
- The participants wondered how they could find which guidewords were used in the graphical result.
- We should develop a set of guidewords/checklists targeted at legal risks.

2.2 Graphical language

- The use of graphical models makes relationships between the different risks etc. much easier to understand than when just reading normal prose.
- The chaining together of threat scenarios to describe more complex scenarios makes for large and complex diagrams which can become hard to understand. This also leads to readability issues as the diagrams need to be scaled down in size to fit on the page. The diagrams should have a clear structure and only be a few levels deep. Often, this is caused by overly general threat scenarios etc. in the diagrams. To remedy this problem, threat scenarios may be combined, or the diagram may need to be split into several more specific diagrams, one for each particular “path” through the original diagram.
- Diagrams where arrows go back and forth are difficult to read and navigate. To improve readability, the presentation of information should be made

linear, i.e. to be read as a “story” from left to right. For instance, going from left to right, one could start with threats, followed by one or two levels of threat scenarios, then unwanted incidents, and finally the assets which are affected.

- The meaning of the different lines used in the CORAS language is confusing (dashed or solid line, with or without arrow). Also, some of the labels are difficult to understand, such as the <<Initiate>> and <<include>> labels used to model relationships between threat scenarios and unwanted incidents. Several modifications have been made to the CORAS language to mitigate these problems, as described in section 5.2.
- From a psychological standpoints, the different icons, in particular the use of “bombs everywhere”, may lead to a very negative impression. This observation has also been made in other settings. The graphical icons used in the CORAS language are currently being revised.
- It should be possible to illustrate the *level of risk* by different means, for instance by changing the colour, shape and size of the diagram elements, such as the threat scenarios, or the thickness of the arrows and lines.

3 Method for model-based legal risk management focusing on trust and security issues in VOs

This method aims to assist organisations to carry out a legal risk analysis in the context of setting up a Virtual Organisation, with a particular focus on trust and security issues.

Risk management is the sum of the culture, processes and structures that are directed towards effective management of potential opportunities and adverse effects. The *risk management process* consists of systematic application of management policies, procedures and practice to the tasks of establishing the context and identifying, analysing, evaluating, treating, monitoring and communicating risks. Risk management thus covers the entire lifecycle of the system or organisation, and may include several risk analyses with different focus areas and abstraction levels as the system or organisation and its surroundings evolve over time. The risk analysis process is typically organised as a set of meetings, as summarised in Figure 1 below.

Meeting 1: Introduction
- Client present the system or organisation they wish to analyse
- Characterise the focus and scope for the analysis, including legal context
- Set up analysis plan

Meeting 2: High-level analysis
- Risk analysts present their understanding of the target of analysis
- Identify assets
- Establish initial threats and vulnerabilities

Meeting 3: Approval
- Target of analysis documentation
- Assign value to assets
- Identify risk evaluation criteria

Meeting 4: Risk identification
- Identify risks through structured brainstorming

Meeting 5: Risk estimation and evaluation
- Estimate likelihood and consequence of risks
- Evaluate risks with respect to risk evaluation criteria

Meeting 6: Risk treatment
- Identify and evaluate treatments

Meeting 7: Finalisation meeting (if necessary)
- Present results and get any missing input

Figure 3 Risk analysis meetings

The risk analysis team consists of a small core group of risk analysis experts, typically a risk analysis leader and secretary. In addition, it includes representatives from the client who wants the analysis to be carried out as well as relevant domain experts, such as experts on the legal aspects being analysed. The goal is to involve people with different backgrounds and different insight into the problem at hand in order to elicit as much relevant information about potential risks as possible. The risk analysis experts and domain experts are often independent from the client of the analysis.

The method in this document describes the steps to be performed by the risk analysis team. The method is based on the CORAS[14] method for security risk analysis, which was slightly adapted to the legal context. Consequently, we assume that the method will work best for legal risk analyses where information security issues are the central element. For analysing legal aspects that are not related to trust & security in an IT context, other methodologies may need to be developed. However, the CORAS method is based on generic risk analysis methods and techniques, and has proven useful in a variety of settings.

In the following sections, we will present the risk analysis meetings and activities in more detail.

3.1 Introduction meeting

The introduction meeting aims at achieving an initial understanding of what the client wishes to have analysed and what kind of risks the client is most concerned about. Some of the questions that should be answered include:

- For whom is the analysis carried out?
- For what purpose do we perform this analysis?
- What do we want to protect?
- What is the scope?

An in-depth analysis can be a time consuming and costly process, and the client typically has limited resources available for risk management. By clearly characterising the target and focus of the study, including identifying what falls outside the scope of the analysis, the available resources can be utilised in the most effective and efficient manner.

During a risk analysis, we make several assumptions and choices with regards to the system or organisation under analysis as well as its surroundings. Documenting these choices and assumptions is necessary for being able to determine in which contexts the analysis results are valid. As the system or organisation and its surroundings change over time, these assumptions may no longer hold true. In this case, the analysis may need to be updated to determine whether the risk level of any of the previously identified risks has changed and to identify any new risks

[14] See http://coras.sourceforge.net/.

which may have arisen. Mechanisms thus need to be put in place to monitor the risks and assumptions and determine when a new risk analysis is necessary.

The introduction meeting should include the risk analysts and the client of the analysis, typically represented by a person with decision making powers with respect to the system or organisation being analysed. The meeting may also involve other stakeholders or parties who have an interest in or knowledge about the system or organisation.

The risk analysts should give a brief presentation of CORAS to familiarise the client with the risk analysis process and some of the methods and techniques which may be used underway, such as structured brainstorming and the graphical language.

3.1.1 Client presents system or organisation

The client presents the system or organisation they wish to have analysed and what kind of incidents they are most worried about. This presentation will typically include a mix of text (prose, tables, etc.), informal diagrams, such as “rich pictures”, and models describing the system or organisation to be analysed. Depending on what the client wishes to analyse, this presentation would normally cover a number of different areas, such as business goals and processes, users and roles, contracts and policies, hardware and software specifications, network layout, and so on.

Figure 4 shows a typical target diagram as presented by the analysis client. This diagram represents a simplified version of the CE VO scenario analysed in D15, depicting the actors and their relationships.

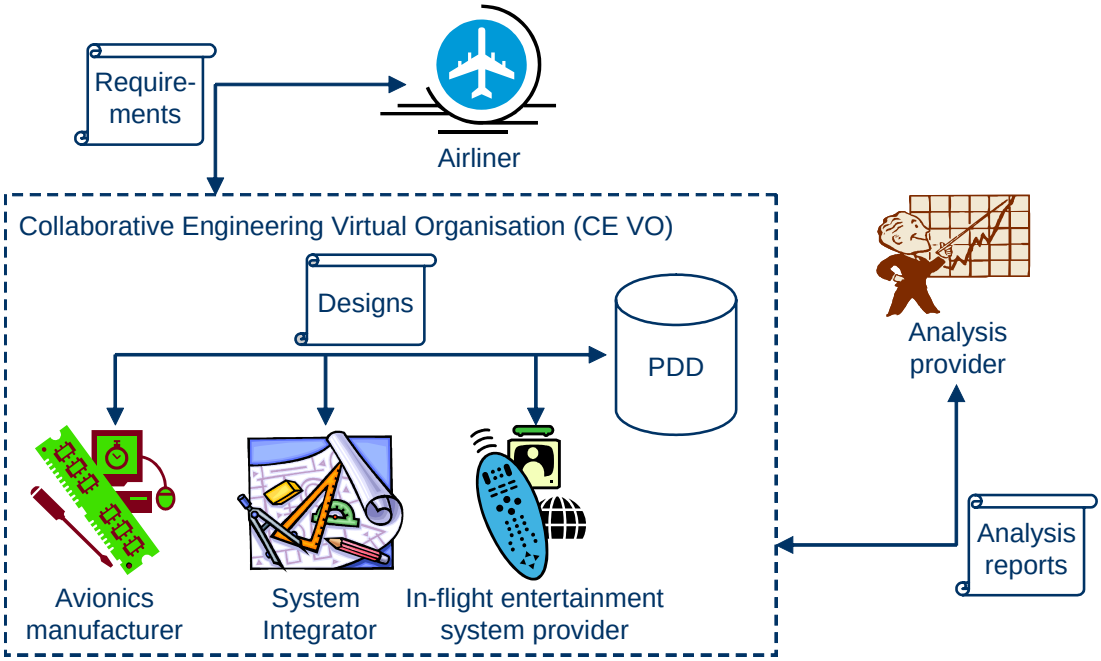

Figure 4 Actors in CE scenario

3.1.2 Characterise focus and scope of the analysis

The client and the risk analysts should characterise the focus and scope of the analysis. Characterising the focus and scope is important to ensure both a common understanding of the problem at hand and to ensure an efficient use of the available resources by focusing on the aspects of the system or organisation that are of real importance to the client. This includes defining the borders between what is to be part of the analysis (target) and what is to be left out. Part of defining the scope is selecting which legal aspects will be covered in the analysis, e.g. confidentiality in relation to business information, data protection law, IPR aspects, etc., along with security aspects, such as confidentiality, integrity and availability, as well as other aspects of interest. The risk analysts should interact with the client to clarify any questions or uncertainties with regards to the target of analysis to avoid misunderstandings later on.

3.1.3 Plan the analysis

Finally, the rest of the risk analysis should be planned in more detail, including identifying participants and meeting times and venues, based for example on the suggested meeting schedule presented in Figure 1 above. To achieve continuity in the risk analysis process it is important that the core group of participants commit to the risk analysis and are able to participate during the whole process so that the risk analysts do not have to interact with new and different people at every meeting. Additional persons may be involved in the different meetings based on the competence which is required.

The risk analysis team typically consists of one or two risk analysts who perform the actual risk analysis. One risk analyst should be responsible for leading the risk analysis sessions, and an additional person may act as a secretary during the sessions, recording the results and assisting the risk analysis leader when necessary.

The analysis team should include a representative of the client with decision making power with regards to the target of analysis. In addition, it should include other stakeholders, domain experts and interested parties with knowledge about the target of analysis, such as system managers, developers, users, lawyers, security experts, and so on. The goal is to involve people with different backgrounds and different insight into the problem at hand in order to elicit as much relevant information about potential risks as possible. If the risk analysis team becomes large, it may be beneficial to split it into smaller groups during e.g. the brainstorming sessions described below. The point is to give everyone a chance to participate and feel useful, as well as to be able to control the group when necessary.

The participants of the risk analysis are documented in the risk analysis roles table, as shown in the example from the CE VO analysis in Table 1 below.

Role	Name	Organisation	Background/Expertise
Risk analysis leader			Risk analysis, security
Risk analysis secretary			Risk analysis, security
Target owner			Aerospace industry
Domain expert			Engineering & design
Domain expert			Intellectual property law
Domain expert			Socio-economy and trust

Table 1 Risk analysis roles

The plan for the analysis is summarised in a risk analysis plan table, as shown in Table 2.

Date	Tasks	Participants

Table 2 Risk analysis plan

3.2 High-level analysis

One of the goals of the second meeting is to ensure a common understanding of the focus and scope of the analysis, as well as to identify the client's main assets in the system or organisation. Assets are central to the CORAS risk analysis method and help guide the entire risk analysis process. The assets are used to assist in identifying risks and estimating their consequences in terms of loss of (monetary) value of the different assets. If the system or organisation does not contain any assets with respect to the client of the analysis, there is nothing that can lose value for the client, and hence no point in a risk analysis. A high level analysis of threats, vulnerabilities and unwanted incidents is performed to help identify what the client is most worried about happening, and thus to ensure a correct characterisation of the focus and scope of the analysis.

3.2.1 Risk analysts present target of analysis

Based on the background documentation from the client and the presentations and discussions from the introduction meeting, the risk analysts start by presenting their understanding of the target of analysis, inviting comments and corrections from the client. This is done to ensure a common understanding of what is to be analysed and what is to be considered outside the scope of the analysis. The target is characterised using for example UML diagrams or other types of models to specify the target and its relations with the surroundings, such as the figures below.

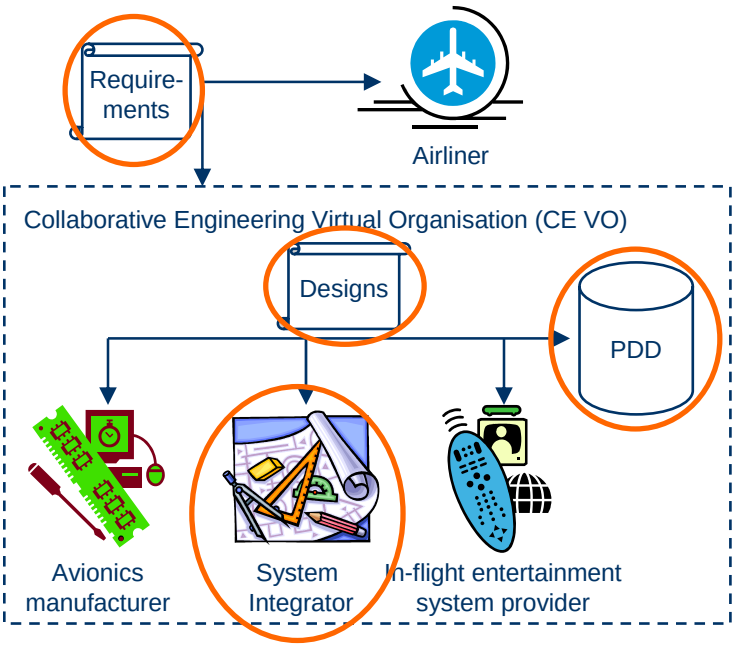

Figure 5 CE VO target of evaluation

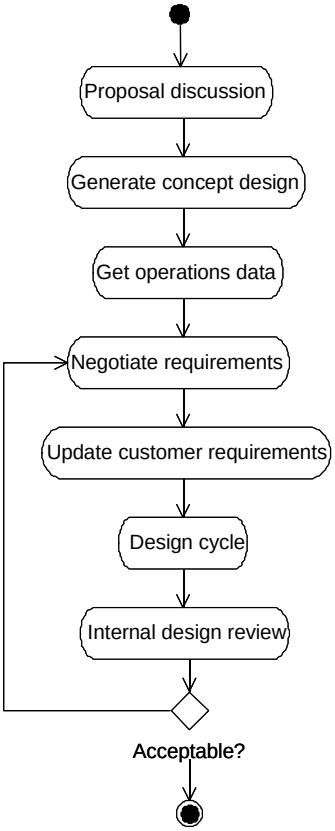

Figure 6 High-level CE VO design process

In a legal risk analysis, particular attention should be given to providing an overview of legislation of relevance to the type of VO to be created, as well as any pre-existing contracts and contracts foreseen between VO members in order to ensure the functioning of the VO. An example of this is shown in Figure 7.

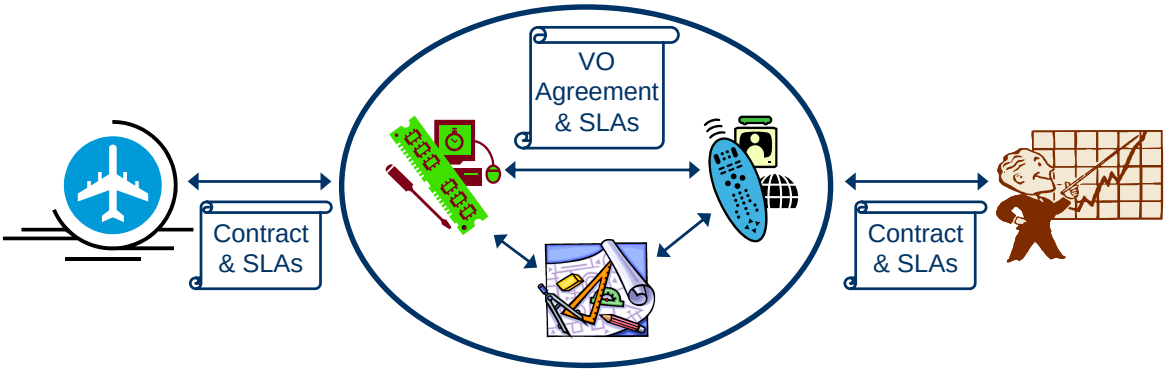

Figure 7 Contracts in CE VO scenario

3.2.2 Identify assets

Assets are the parts or features of the target of analysis that have value to the client and that the client wants to protect, such as physical objects, key personnel, services, software and hardware, or more intangible things such as know-how, trust, market share and public image. By directing the analysis towards the assets of highest value to the client, one ensures that the available resources are spent on identifying the risks of highest impact on these assets. If the target contains no assets of value for the client, there is nothing that can be harmed and lose value, and hence no point in a risk analysis. If applicable, point out how the assets are legally protected, e.g. through intellectual property rights (IPR).

The risk analysts typically perform an initial identification of assets based on the information provided by the client in presentations and target documentation. During the meeting, the list of assets is discussed and updated together with the client. To limit the size of the analysis, the number of assets shouldn't grow too large, typically the 4-6 most important assets suffice.

3.2.3 High-level risk analysis

Sometimes it may be difficult to identify exactly what should and should not be included in the risk analysis. Furthermore, the client is often tempted to include as much as possible. However, the result of this may be to analyse nothing at all in sufficient detail due to lack of time and resources for the analysis.

A preliminary high-level analysis of the target may be performed to identify the most important threats, vulnerabilities and unwanted incidents to ensure that the focus of the analysis will be on the risks that the client is most worried about. The results of this analysis may help refine the focus and scope of the analysis and serve as a basis for further work during the risk identification activity.

This high-level analysis may utilise the same techniques for risk identification as described in the following sections, but more informally. For example, one could use structured brainstorming as described in section 3.4 below to identify focus areas but leave out the more detailed analysis of likelihood and consequence of the identified risks. The results of the high-level analysis may be documented in a table such as the one below.

3.3.2 Asset values

After identification, the assets should be ranked relative to each other based on value or importance to the client, in order to facilitate estimating consequence values and prioritising the risks. Not all assets can be measured in monetary value, such as human life and health. In these cases, other criteria for risk evaluation may be needed, cf. section 3.3.3. The assets should be documented in an asset table, such as the one shown in Table 4.

Asset ID	Description	Asset category	Asset value

Table 4 Asset table

3.3.3 Risk evaluation criteria

The goal of this activity is to determine what level of risk the client is willing to accept, in terms of what loss in asset value can be tolerated over a given time interval. Risk level is expressed in terms of likelihood, i.e. what are the chances of this risk occurring, and consequence, i.e. what is the loss with regards to the asset which is affected by the risk. The likelihood and consequence values can be expressed in terms of quantitative values, such as statistical probability or amount of money lost. However, often we do not have the necessary data needed to calculate accurate values, for example through statistical analysis. Instead, we use qualitative values for likelihood and consequence, e.g. low, medium and high, together with examples illustrating what these values mean.

The risk evaluation criteria specify what level of risk the client is willing to accept, and should be expressed in terms of the likelihood and consequence values defined above. Based on the consequence and likelihood, a risk may be either accepted, or it is selected for further evaluation and treatment. Typically, this can be done by setting up a matrix which shows the mapping of consequence and likelihood values to either “accept” or “evaluate”, as shown in Table 5.

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Rare					
	Unlikely					
	Possible					
	Likely					
	Certain					

Accept

Evaluate

Table 5 Typical risk matrix

3.4 Risk identification

This meeting seeks to identify the risks to be managed, i.e. where, when, why and how incidents could prevent the achievement of objectives or reduce the value of an asset. The activity makes use of selected techniques and elements of conventional risk analysis methods which have been adjusted to fit the model-based approach of CORAS. The risk identification session is organised as a structured brainstorming, inspired by HazOp – Hazard and Operability Analysis (Redmill et. al., 1999).

The goal is to involve people with different backgrounds and different insight into the problem at hand in order to elicit as much relevant information about potential risks as possible. In addition to the risk analysts and the client, the meetings should include people with an interest in and knowledge of the system or organisation under analysis, such as security experts, lawyers, users, system managers, and so on.

Based on the identified assets, models describing the target, and the threats and weaknesses identified by the high-level analysis, the risk analysts should prepare the session by first selecting suitable models as a basis for the analysis, such as use cases, network diagrams, and so on, that match the desired level of abstraction. These should be illustrated using e.g. UML class, sequence or activity diagrams. The risk analysis leader should also prepare for vulnerability identification by selecting suitable checklists. The background documentation should be sent out to the whole risk analysis team prior to the meeting.

3.4.1 Structured brainstorming

This activity is organised as a structured brainstorming. The risk analysis team tries to identify scenarios describing how a threat exploits a vulnerability, leading to an unwanted incident which may reduce the value of one or more assets. The risk analysis leader uses the assets of highest value in conjunction with the diagrams of the target to guide the threat identification process, e.g. by asking relevant questions to the risk analysis team. The use of graphical diagrams also helps understanding and communication between the participants. The identification of threats and vulnerabilities may be supported with the use of pre-defined questionnaires and checklists. This process is illustrated in Figure 8.

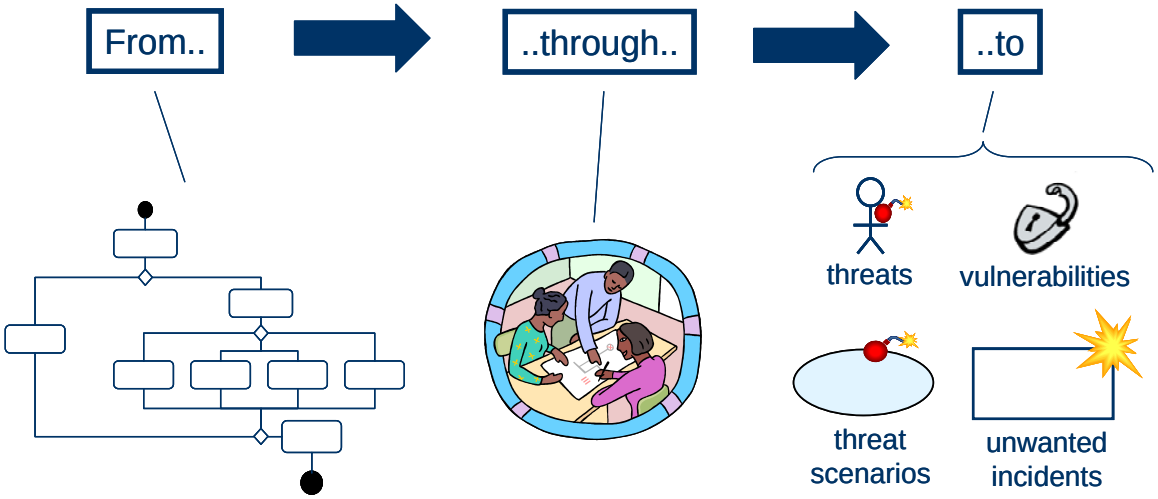

Figure 8 Model-based structured brainstorming

Vulnerabilities can be thought of as control mechanisms that ideally should be in place, but for some reason are missing or not sufficiently robust. Using this metaphor, vulnerabilities can be regarded as unsatisfactory controls, or exceptional circumstances that have not been planned for or that nullify the effect of existing, satisfactory, controls. Vulnerabilities can also be system characteristics that are impossible to treat; an internet connection that is crucial to the system, for example. Identifying new vulnerabilities is often a matter of finding the “blind spot”. It is usually necessary to consider all aspects of the target, e.g. the organisational, judicial, physical, and computational characteristics and compare these findings with the relevant policies.

During the meeting, one person from the risk analysis team should have the responsibility to record and document the results of the structured brainstorming. Following the risk identification meeting, the risk analysts structure the results and document the findings by the means of threat diagrams as defined in the CORAS graphical language. These diagrams are used later on as a basis for estimating the risk level as well as for identification of treatments. In the CORAS language, a threat, e.g. a disloyal employee or a computer virus (typically represented in the diagram by a stick figure), is related to a threat scenario, which is a sequence of events or activities leading to an unwanted incident. A vulnerability may be attached to this relation. An unwanted incident is an event resulting in a reduction in the value of the target asset. Furthermore, an unwanted incident may initiate or lead to other unwanted incidents, forming chains of events.

The risk analysts should also assess the need for further threat or vulnerability identification. For each unwanted incident the risk analysts should decide whether it is described at an appropriate level of abstraction, or whether additional analysis is required. The reason for the latter could be the need for more detailed incidents to make the assignment of frequencies feasible, or that the unwanted incident seems to require high priority. Additional information may be elicited from the client or other participants of the risk identification session, or the risk analysis leader may

determine that an additional risk identification meeting is needed, but this time focusing on a smaller part of the target of analysis.

3.5 Risk estimation and evaluation

As mentioned in section 3.3 above, the client does not have unlimited resources to implement risk reducing measures. We therefore need to prioritise the risks and select a subset of them for further attention and treatment. Risk estimation is the systematic use of available information to determine how often specified events may occur and the magnitude of their consequences. A *risk* is an unwanted incident along with its estimated likelihood and consequence values. These values are the basis for risk evaluation. The goal of the risk evaluation is to prioritise the risks and identify which ones are in need of treatment by comparing against the pre-established criteria, as described in section 3.3.3.

3.5.1 Estimate risk level

The goal of this activity is to estimate the level of risk for the identified unwanted incidents. This consists of evaluating the likelihood and consequence of the incident. The consequence is a measure of loss of asset value when the incident occurs, while the likelihood is a measure of how often an unwanted incident occurs. Input to the likelihood and consequence evaluation is the threat diagrams produced based on the results from the risk identification meeting. These document the identified threat scenarios, and may also contain consequence values which have been provided by the risk analysis team during the risk identification.

The methods chosen for consequence and likelihood evaluation depend on the results from the risk identification, the historical and statistical information available, and the analysis group's ability to assign consequence and likelihood values. In many cases, estimates are elicited from the client, domain experts or other people with knowledge of the target of analysis. If statistical or historical data is available, more sophisticated methods may be used, for instance Fault Tree Analysis (IEC, 1990) for calculating the frequency of an incident.

The risk analysis leader presents the threat diagrams created from the risk identification meeting, as described in section 3.4.1 above. For each diagram, consequence and likelihood values are estimated for the different threat scenarios and unwanted incidents, based on expert judgements made by the system owner in collaboration with the risk analysis team. The results are documented in a consequence and likelihood table, as the one shown in Table 6.

Risk ID	Asset	Unwanted incident	Consequence	Likelihood

Table 6 Consequence and likelihood table

3.5.2 Evaluate risks

The risk evaluation compares the estimated risk level against the pre-established criteria which were identified in the approval meeting, as described in section 3.3.3 above. This enables a prioritisation of risks, which is the basis for the subsequent decision about which risks should be targeted for treatment. Note that we may not be in a position to treat all risks, depending on the resources available for establishing risk reducing measures.

Prior to the evaluation, risks may be grouped or categorised. This categorisation can be done according to different concerns, for instance to group risks which have similar treatment options and thus reduce the work necessary for treatment identification and evaluation.

We then apply the risk evaluation criteria specified earlier during the approval meeting. After estimating the likelihood and consequence of the risks, they may be plotted into the pre-established risk matrix, described in section 3.3.3 above.

3.6 Risk treatment

This phase aims at treating the non-acceptable risks by developing and implementing specific cost-effective strategies and action plans for reducing the risk level.

3.6.1 Identify treatments

For each risk which is not accepted, potential treatment options are explored in a similar manner to the structured brainstorming used for risk identification. This session typically involves the same participants as the risk identification. A walkthrough is performed of the CORAS threat diagrams created from the risk identification sessions, and the participants are asked to come up with suggestions for different ways to reduce the risk.

There are four main approaches to risk treatment:

- Reduce the likelihood of the incident occurring.
- Reduce the consequence if the incident should occur.
- Transfer the risk to another party, e.g. through insurance or outsourcing. This option will be of particular relevance in a legal context. VO partners should assess whether risks affecting one partner need to be shared by the others, e.g. though a consortium agreement. If insurance is available, the VO may consider transferring the risk to an insurance company.
- Avoid the activity leading to the risk.

The outcome of the treatment identification is documented using the CORAS graphical language by adding treatments to the existing diagrams. The type of treatment is specified according to the main approaches listed above, e.g. <<ReduceLikelihood>>.

3.6.2 Evaluate treatments

To determine the best expenditure of the resources available for risk reducing measures, the identified treatments are evaluated with respect to their usefulness. The degree to which the treatment reduces the level of risk is estimated, and a cost/benefit analysis is performed. Based on these results, the treatments can then be prioritised and implemented based on the available resources.

3.7 Finalisation meeting

For the risk analysis to have value, the findings of the risk analysis also need to be communicated to the relevant stakeholders to raise awareness and to ensure that relevant measures are put in place to prevent harmful events from occurring. In addition, the results may provide important input to future analyses, serving as a starting point and avoiding the need to start analysing from scratch every time.

The content of this meeting, and whether it is held at all, depends on how the client wants the findings of the risk analysis to be presented. To cut down on costs, the client may forego a written report in favour of a slide presentation of the main findings. Other clients want a written report, or a combination of both.

4 Legal checklist

The objective of this checklist is to facilitate legal risk management in relation to an enterprise network (EN) or a virtual organisation (VO). The EN is created with the general purpose to facilitate the set-up of VOs within a defined domain. The individual VOs are then created in order to serve a particular purpose, e.g. in the TrustCoM context, to provide learning services to a learning citizen as specified in the agreed learning path.

The checklist aims to point out selected issues of particular relevance (1) to the internal (B2B) relations within a network and (2) to the relation between the network or one of its members, and an eventual customer who may be a consumer or a business (b2c or b2b). The checklist only mentions issues, without analysing them in any detail. More detailed analyses of the issues are included in other parts of this report and in other TrustCoM reports.

This list of possible legal issues may be used to identify risks and to identify areas that should be regulated in contracts. When creating an enterprise network or a virtual organisation, the founding parties will first need to discuss a strategy for the network and a governance structure, which is necessary in order to ensure the functioning of the VO. This strategy is largely to be guided by the goals the parties have for their network. The checklist therefore also mentions issues to be considered regarding this governance and management structure of the network. A risk management process can first be started once one has agreed upon a basic plan and an initial governance structure for setting up an EN.

The usefulness of this checklist will differ from one application scenario to another. The list was developed with the TrustCoM eLearning scenario in mind. For other EN/VO scenarios, some of the issues may not be relevant at all (e.g. eMarketplace issues or consumer law issues), while other issues may need to be addressed in addition (e.g. specific issues relevant for the aerospace industry in the TrustCoM CE scenario). The current checklist should therefore be supplemented by other, industry-specific checklists.[15]

---

[15] Available legal checklists include the following:

a) Sixth Framework Programme Checklist for a Consortium Agreement
http://europa.eu.int/comm/research/fp6/working-groups/model-contract/pdf/checklist_en.pdf

b) Electronic Commerce and Technology Transactions Checklist (US law)

http://www.ffhsj.com/bancmail/ftcintro.htm

c) VO-related checklist: The VE Interchange Agreement (ALIVE project deliverable D 17)

http://www.vive-ig.net/projects/alive/Documents/VE_Interchange_Agreement.zip

d) Checklist for selecting an electronic marketplace:
http://www.emarketservices.com/templates/Page____431.aspx.

e) Chapter on contracts in Jon Iversen, *Legal risk management,* Thomson, København 2004.

4.1 EN or VO Internal Relations

The following issues should be considered when setting up an Enterprise Network or a VO and when drafting a contract for such a network:

1. EN/VO Governance
    a. Legal Form
        i. Joint Venture
        ii. Partnership
        iii. Company (Ltd.)
    b. Control & Management
    c. Decision Making & Voting in EN/VO
    d. Internal Controls
    e. Partners' Contribution to EN
    f. Pricing
    g. Performance Standards
    h. Exclusivity
    i. Operating Rules
    j. Process for Amending EN Governance Rules
2. EN as a Marketplace for Services
    a. Marketplace Owner
    b. Does the Marketplace Owner Provide Competing Services on Marketplace?
    c. Neutrality of Marketplace Owner
    d. Financial stability of the Marketplace
3. Validity and Enforceability of Contract
4. Financial Issues
    a. Profit/Loss Sharing
    b. Financial Responsibility of Parties
    c. Taxation
5. Liability
    a. Liability Allocation
    b. Limits of Liability
    c. Force Majeure
    d. Insurance
6. Technical Issues
    a. Authentication
    b. Encryption
    c. Security
    d. Technical Risk Management
    e. EDI (Electronic Data Interchange Agreements)
    f. Electronic Agents
    g. Records keeping
7. IPR & Confidentiality
    a. Patents
    b. Trademarks
    c. Domain Names

   d. Design
   e. Copyright & Database Rights
   f. Know-How
   g. Confidentiality
   h. IP Protection
   i. Works brought into EN/VO
   j. Works created during course of EN/VO
8. Data Protection
   a. EN Member Access to Personal Information
   b. EN Member Use of Personal Information
   c. Trans-border Data Flow
   d. Safe Harbour Rules
9. Trust Management
   a. Defamation
   b. Data Protection
   c. Confidential Business Information
10. International Aspects
   a. Choice of Law
   b. General Jurisdiction
   c. Targeting
   d. Corporate Residence
   e. Taxation
11. EN and VO Membership Management & Lifecycle Issues
   a. Eligibility for Participation
   b. Contract Duration & Dissolution
   c. Integration of New Members
   d. Subcontracting
   e. Changes in VO Participation
   f. Expulsion/withdrawal from VO or EN
   g. Dissolution of VO or EN
   h. Modification of VO agreement
12. Dispute Resolution and Arbitration

4.2 The Relation to the End-User

1. End-User Authentication & Identification
   a. Consumer Identity
   b. Choice of Identity Management Framework
   c. Use of Passwords
   d. Use of Biometrics
   e. End-User Anonymity
2. Privacy/Data Protection Law
   a. Is Personal Information Collected?
   b. Methods of Collection
   c. Exchange of Personal Data within EN
   d. Access to Personal Data within EN

    e. End-User Access to Information
    f. Data Quality
    g. Identity Theft
    h. Children's Online Protection
    i. Data Retention and Destruction
3. Security
4. Access to Content
    a. Type of Content
    b. Duration of Access
    c. Requirements to User’s Computing Infrastructure
5. Consumer Laws
    a. Accessibility for Users with Special Needs
6. International Aspects
    a. Choice of Law
    b. General Jurisdiction
    c. Targeting

5 Graphical language for legal risk management

Risk analysis requires a clear understanding of the system or organisation to be analysed. This can only be achieved through the involvement of stakeholders with different backgrounds and knowledge about the system or organisation being analysed, e.g. security experts, legal experts, system owners, developers and users. The effectiveness of the analysis depends on the extent to which the participants are able to communicate with and understand each other. The CORAS graphical language for threat modelling has been designed to mitigate this problem within the security domain.

During the legal risk analyses we have performed of the TrustCoM test bed scenarios we have utilised the graphical language as well as other UML mechanisms to document and analyse legal risks, as documented in TrustCoM Deliverable 15 appendix A, B and C and Deliverable 17 appendix B. Through these analyses, the current language has proven a good starting point for legal risk analysis. However, we see the need for several changes to better suit the needs of legal risk analysis. Appendix E of D15 presents a number of requirements for the user-level language for legal risk analysis, such as:

- The language should support legal risk analysis.
- It should be possible to model both input and output of legal risk analysis.
- The language should be easy to understand and use by all participants in legal risk analysis.

This chapter describes the changes and extensions which have been made both to the graphical language and the Unified Modelling Language (UML) in order to make them more suitable for analysis, documentation and communication of legal risks. The chapter is divided in two. First we discuss the use of UML for modelling the input to the legal risk analysis, e.g. modelling contracts and legal concepts such as ownership, permission, etc. In the second part, we discuss the changes which have been made to the graphical language for documenting the output of the risk analysis.

Work has also been done on defining the semantics of the extended languages, in order to achieve a clear and precise understanding as well as to facilitate automated tool support. This work is detailed in TrustCoM report D15 appendix E.

5.1 Modelling legal aspects using UML

CORAS uses graphical models of the target of analysis, i.e. the system or organisation being analysed, in order to facilitate understanding and to guide the analysis. Different modelling languages may be used, however we typically use various types of UML diagrams. In a security risk analysis, we may for example use UML class diagrams to model the structure of the system or organisation and sequence or activity diagrams to model behaviour. However, we wish to be able to

model and analyse more legal aspects, for example whether the act of disclosing certain information is forbidden by contract, e.g., by a non-disclosure agreement. To enable this, we need facilities for:

- specifying ownership, which is highly relevant when determining e.g. the rights and obligations of an actor,
- specifying legal effects on different roles and activities, and
- correlating these effects with the relevant legal sources, e.g. which contract clause is the source of the legal effect in question.

Input to a legal risk analysis includes not only system descriptions and the like, but also laws, contract clauses, obligations and permissions, and so on. The extensions to UML for modeling these aspects are detailed in D15 Appendix E, however we give some examples below. Modal logic, in particular deontic logic, has

the likelihood of a threat scenario, not vice versa). In addition, we have added the ability to model that the treatment itself may cause other threat scenarios or incidents to happen, by adding an arrow from a treatment to a threat scenario or unwanted incident. For example, a treatment for excessive e-mail spam may be installing anti-spam software, but this may also lead to the new threat scenario of rejecting non-spam e-mail messages, as shown in Figure 15. As all arrows now represent <<Initiate>> relationships, the <<Initiate>> stereotype tag is superfluous and has been removed from the diagram to make it less cluttered.

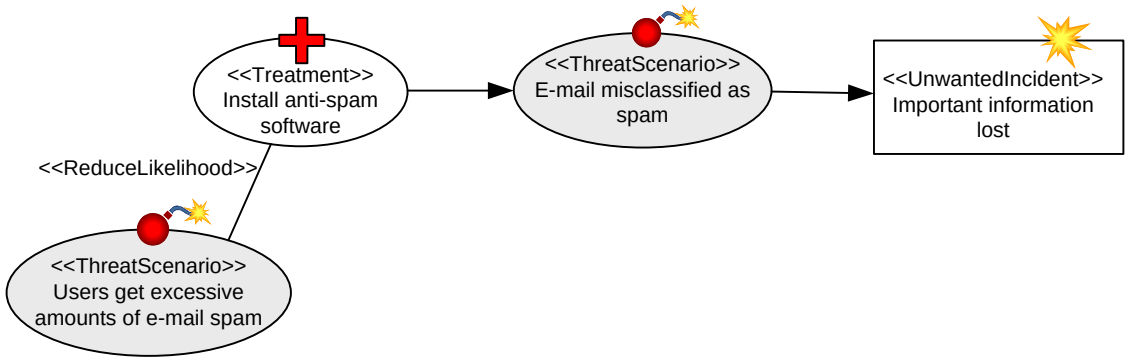

Figure 15 Treatments may initiate new threat scenarios

The way vulnerabilities are documented has also changed. In the original language, vulnerabilities were recorded along with asset they affected. However, this made it difficult to see the relationship between the threats, vulnerabilities and treatments. Furthermore, the vulnerability might be recorded multiple times, once for each asset it affects. Instead, vulnerabilities are now positioned directly on the relevant <<Initiate>> relationship where they are being exploited in order to lead to a new threat scenario or unwanted incident.

Some of the changes deal more with the graphical representation of elements in the language. The use of different types of arrows in the original CORAS language has been a source of confusion. The original language used dashed arrows between the different use cases, such as threat scenarios and treatments, but solid lines between the use cases and the actors, e.g. threats and assets. This is a legacy from UML use case diagrams. The arrows have been changed to use solid lines instead, as well as more prominent arrowheads to make the direction of the arrow more easily visible. Furthermore, the unwanted incidents are now modelled using a box rather than an oval. This is motivated by the link to UML use case diagrams where ovals represent scenarios, whereas an unwanted incident is rather regarded as a single event. The graphical icon representing an unwanted incident has also been changed from a kind of warning sign to an “explosion”, which is more closely related to the bomb symbol used for threats and threat scenarios. The text related to the threat scenarios, treatments and unwanted incidents are now put inside the ovals and boxes. This both saves space and makes the diagram look less cluttered. Some colors have also been changed to improve readability, e.g. the oval representing a threat scenario has changed to a lighter shade of grey.

As described in section 2.1, Fault Tree Analysis was not very useful in the legal analysis due to the lack of data for a statistical analysis. However, the fault tree

diagram mechanisms were seen as useful for structuring incidents and modelling more complex relationships. This has led to the inclusion of facilities for modelling 'AND' and 'OR' relationships in the graphical language. An example fault tree diagram based on the CE VO risk analysis in deliverable D15 is shown in Figure 16. A diagram displaying similar information using the new 'AND' and 'OR' relationships in the updated graphical language is shown in Figure 17.

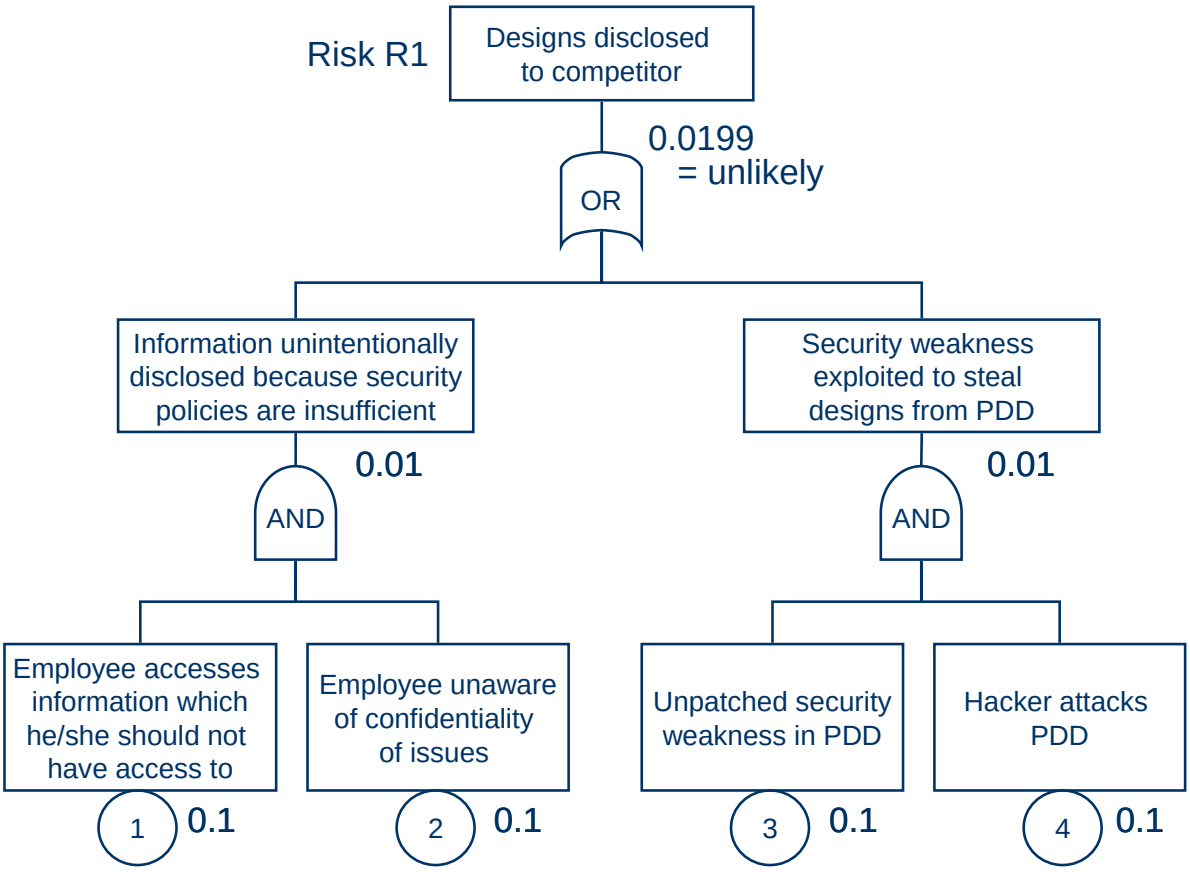

Figure 16 Original fault tree diagram

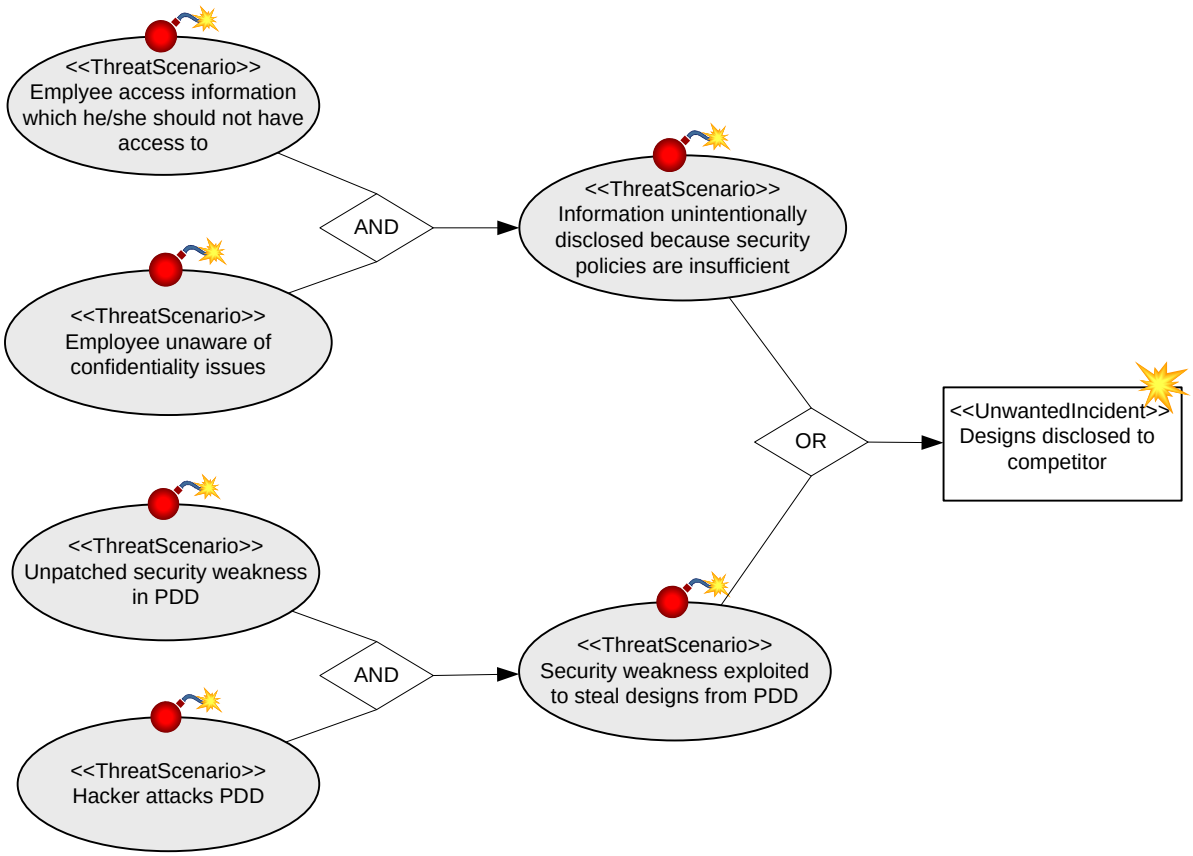

Figure 17 Example of use of 'AND' and 'OR' relationships in graphical language