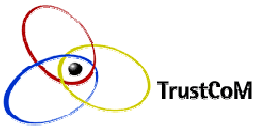

Deliverable

60

Appendix A

Legal risk analysis of confidentiality issues in the CE scenario

WP9 Legal Issues

Author: Tobias Mahler,
Dana Irina Cojocarasu
Organisation: NRCCL
Date13.07.2006
Version 1.0

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

Disclaimer

This document is the result of research work carried out in the TrustCoM Project. It is not intended to be legal advice and is not to be construed or understood as legal advice. Persons interested in applying any information in this document to their specific needs are recommended to seek relevant professional legal advice regarding their specific needs/requirements.

Neither the authors of this document, nor the TrustCoM Consortium, nor the European Commission shall be liable for any use made of this document. This document does not represent the opinion of the European Community nor is the European Community responsible for any use that might be made of the content of this document.

Forum

Any dispute arising out of or in connection with this document shall be submitted to the exclusive jurisdiction of the Norwegian Courts.

Table of contents

1 Introduction

This appendix to TrustCoM report D 60 contains a legal risk analysis of the TrustCoM CE scenario. The appendix should be read in connection with the main report, which analyses legal issues in relation to confidentiality agreements. In the following, we will exemplify based on the CE scenario how confidentiality issues may be proactively analysed and addressed.

The appendix is structured as follows: Section 2 synthesizes the storyboard of the TrustCoM CE scenario, which was the basis for this case study. Section 3 presents the methodology utilized in this case study. The analysis of the scenario is presented in the subsequent sections. Section 4 presents the risks; Section 5 discusses the different options to treat these risks. Section 6 and 7 respectively discusses how these risk treatments can be transformed into contract requirements and contract drafts. Finally, Section 8 summarizes the findings of this risk analysis as well as the findings of the main report in a check list of risks related to confidentiality issues.

2 TrustCoM CE Scenario description[1]

The objective of this case study is to analyse the risks related to confidential information in the CE scenario from a legal point of view and to identify means that can contribute to effective risk reduction. The focus for the analysis will be on the interactions and contracts between the CE VO and the following partners: TC-ConsEng, TC-SP and TC-HPC as explained below.

The TrustCoM CE application testbed uses a collaborative engineering scenario set in the aerospace industry. The background is collaboration between different partner organisations, e.g. in a joint venture, to design, build and maintain an aircraft. The design processes involve bringing representatives of the partner organisations to work together and to share data and computational resources with each other, using specialist design houses and computing centres. Particular considerations here are flexible fine-grained access control and protection of proprietary data.[2]

A description of the CE scenario can be found in TrustCoM Deliverable D 41[3].

The scenario involves a consortium of engineering companies CE VO involving a number of 'tier-1' partners who provide major sub-systems to a business jet (such as airframe, engines, avionics etc) who following negotiations with an existing customer receive the task of upgrading an aircraft fleet to support Internet access in the passenger cabin. This involves installing new antenna and communications systems into existing aircraft.

[1] In accordance with TrustCoM Deliverables D10 "Baseline Prototype infrastructure for the CE Scenario" and D41 Enhanced Prototype CE Testbed".

[2] P. Kearney, Trust and security in virtual organisations, BT Technology Journal, forthcoming.

[3] Deliverable D 41, WP35, "Enhanced CE Test Bed", Section 5. The Document makes reference to TrustCoM Deliverable D10, "Baseline prototype infrastructure for the CE Scenario" .

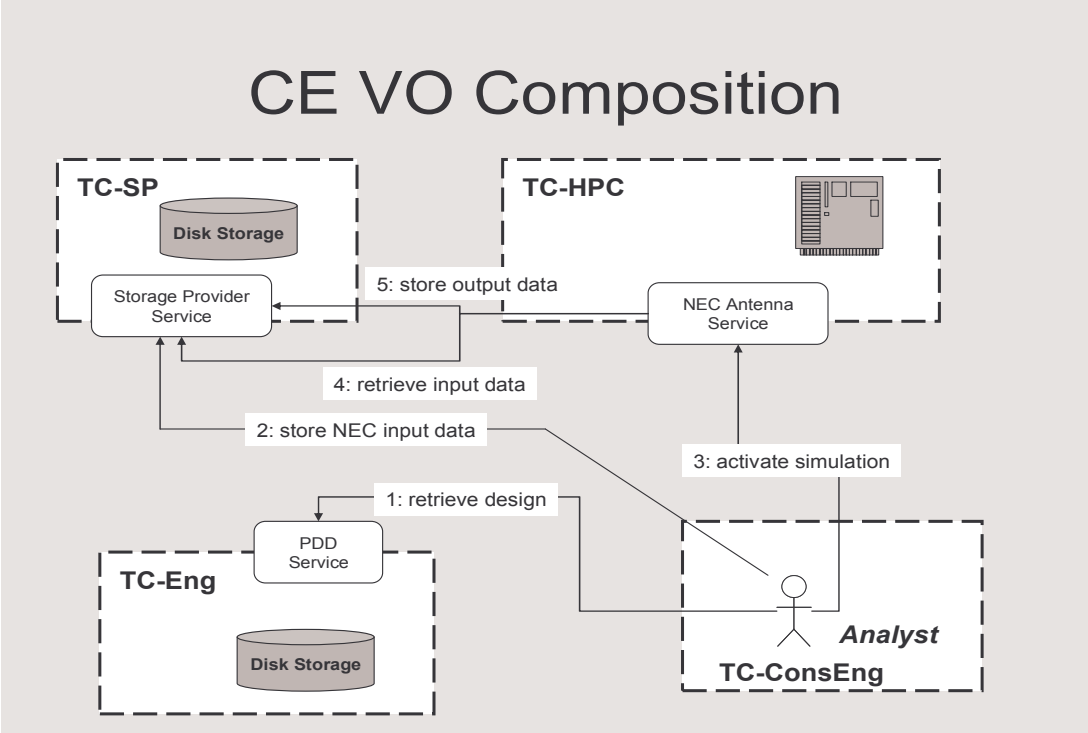

Figure 1 CE VO interactions and information flow

The consortium enrols a new member that has the technical expertise and contacts required for delivering the Internet system (TC-ConsEng). During the scenario, there is an increased demand for High Performance Computing and storage facilities that are required for performing the large-scale simulations of the new antenna and communications systems. Providers of these resources (TC-HPC and TC-SP) are found and join the VO as temporary members. The service providers are intended to work together in the context of a simulation or 'job' that involves the retrieval of design model data from a provider that stores the model input data, the computation of the analysis results by the provider of HPC-based application services, and their storage on an alternative provider of analysis results.

The trust-based security framework ensures that operatives with the role 'Analyst' in TC-ConsEng are able to access the HPC service and the storage provider services with appropriate trust credentials that are acceptable to the partners. The security framework also ensures that there is a delegation of the client's rights to the application services. In this particular case, it means that the HPC service can access the two storage provider services using the access rights of the client.

Figure 1 describes the top-level CE-VO interactions and the information flow whereas Figure 2 illustrates the actors involved in the scenario and their main business roles.

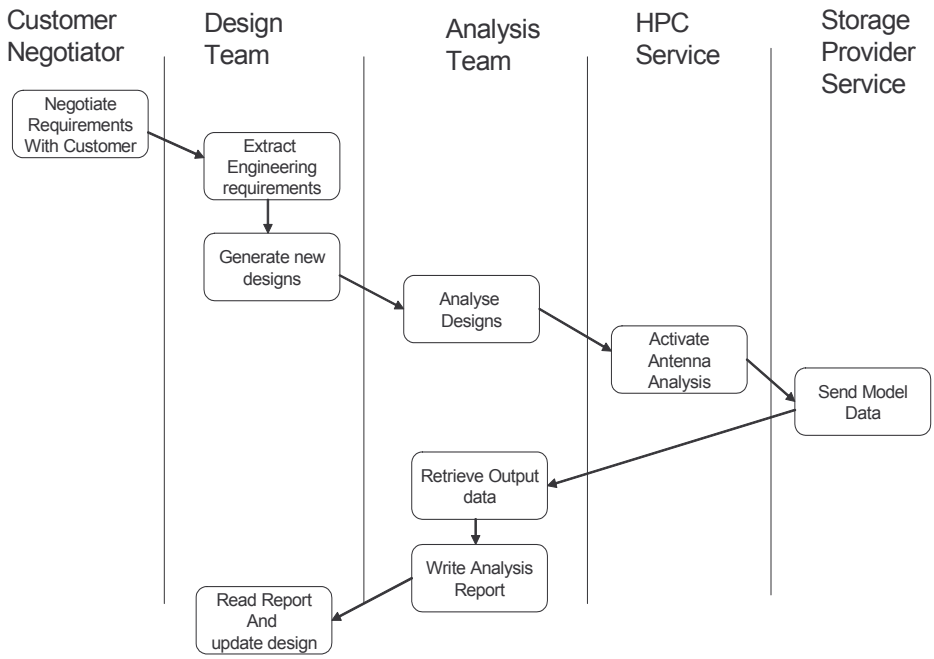

Figure 2 . The Top-level collaborative business process in the CE Scenario

3 Methodology

The methodology utilized for this case study is amended from the methodology presented in TrustCoM report D17 Appendix A. The methodology was adapted in two directions. Firstly, the aim to address confidentiality issues from a legal perspective required us to make a more explicit analysis of the legal protection of confidential information in the first stage of the analysis. Secondly, the methodology presented here puts more emphasis on how the identified risks can be treated within the context of a contract. The methodology presented in D 17 merely spoke of treatment identification, and the concrete steps between the abstract treatment identification and the writing of the contract were not described. This is amended in the methodology that will be presented below, where also the phases subsequent to the treatment identification are explained.

3.1 Select relation

As an initial step, we select the specific relation between VO partners for which the analysis is required. This relation should be sufficiently described with respect to the planned business processes and focus in particular on the information flow (e.g. in UML). The focus of this methodology is on risks to confidential information. Hence, the risk analysts need to identify what kind of confidential information the stakeholder envisages to disclose in the planned collaboration as well as any intellectual property rights that may become relevant during the VO collaboration. It is crucial for the possibility to identify and value risks to these assets that the analysts clarify the legal protection of the information assets involved in the VO information flow.

3.2 Identify, estimate and evaluate risks

The risk identification, estimation and evaluation follow the methodology described in report D 17 Appendix A, with some minor adaptations. In particular, the typical risks to confidential information may in many cases be identified based on a suitable checklist[4] making an inventory of typical risks for particular classes of information assets. For confidential information, typical risks include the possibility of illegitimate disclosure of confidential information to a third party and the misuse of the confidential information by either a business partner or a third party. It is of course important to verify if these typical risks apply in a specific situation. Moreover, possible VO specific additional risks (legal and relevant non-legal) need to be identified. All the identified risks may then be documented utilizing CORAS language, as described in D 17. The risk estimation (determination of risk value, which involves trust assessment) and the subsequent risk evaluation follow the methodology laid down in D 17.

[4] A checklist is included in Section 8 of this Appendix.

3.3 Risk treatment through contractual requirements

Once the risks to the information assets have been identified, estimated and evaluated, the stakeholder of the information asset will seek to identify possible treatments. Since the focus of this report is on confidentiality clauses in VO contracts, these risk treatments should be expressed as contract requirements. The underlying assumption in using the term "requirements" is that the drafting of a contract from a systems theory perspective may be understood as the development of a system of contract rules. If this is the case, the legal discipline may be able to adopt elements of the advanced methods of system development.

As such, it may be possible and useful to define some requirements to a contract, before actually drafting the contract itself. This would e.g. allow us to utilize the systematization of quality requirements developed for IT systems. In IT systems, quality requirements can be categorized based on the distinction of functional and non-functional requirements[5]. While the functional requirements express the desired behavior of a system, the non-functional requirements contain additional quality criteria, which should be taken into account. These non-functional requirements are (based on Grandy 1992) the following: usability (for users), reliability (failure, recoverability, predictability, accuracy), performance (e.g. response time) and supportability.

For contracts, the distinction of functional and non-functional requirements seems not entirely unfamiliar: In fact, the functional requirements describe the functions of a contract. This should include both the achievement of a goal (e.g. receive payment for a service) and to management of risks that are inherent in the situation that should be addressed by the contract (e.g. liability for non-fulfillment). In addition, the contract should fulfill a number of requirements which exceed its mere functionality. These seem to be somewhat parallel to the functional requirements which are well-understood for IT systems. These non-functional quality requirements may also be expressed as the absence of some specific risks arising from how the contract is specified. The non-functional requirements to contracts include the following:

- Usability (risk: only lawyer can read contract)
- Reliability (risk: the contract does not allow determination of rights and obligations)
- Performance (risk: contract procedures are too costly)
- Supportability (risk: contract not amendable, despite changes in circumstances)

In addition to the functional and non-functional requirements, there seem to be some specific additional external requirements of relevance to the legal domain:

[5] Robert Grandy, Practical Software Metrics for Project Management and Process Improvement, Englewood Cliffs, NJ: Prentice-Hall, 1992, p. 32.

- Validity (risk: contract invalid)
- Enforceability (risk: one or more clauses not enforceable).

Hence, this list of contract requirements may be utilized in order to define more specific contract requirements for the VO contract, in order to ensure the management of risks related to confidential information. However, one needs to keep in mind that the fulfillment of requirements may be costly and that some requirements may not effectively mitigate the identified non-acceptable risks. Hence, a cost-benefit analysis should be performed, which should then result in a prioritized list of contract requirements, based on their cost-benefit in relation to the identified most severe risks. This list may then be utilized as a negotiation strategy for the contract negotiation.

3.4 Contract draft

Based on the contract requirements and the negotiation strategy, a contract draft can be put in writing.

3.5 Contract negotiation

The final phase will involve the negotiation of the final contract with the prospective contractors, following the negotiation strategy.

4 Risk identification

The following section describes the identified risks, including vulnerabilities, threats, unwanted incidents and the affected assets. All risk scenarios were assessed from the perspective of the stakeholder of this analysis, i.e. the CE VO.

4.1 Assets

The collaboration between the partners in this business scenario will involve information assets already having or requiring different legal protection (see, D 15 Appendix A p. 26). Therefore, in the context of the present analysis we will only focus on the confidential information involved in the business collaboration.

The legal protection of confidential information is described in the main report of D 60.

4.2 Risk 1: Loss of legal protection

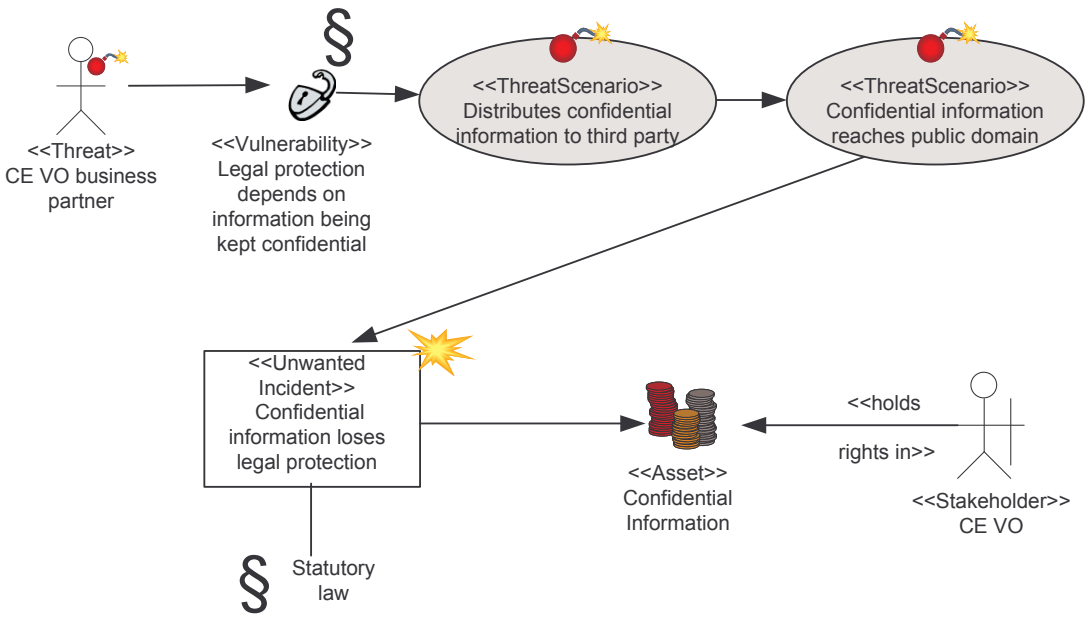

Figure 3 Confidential Information Loses Legal Protection

The CE scenario involves a considerable flow of confidential information between the actors involved, e.g. airplane design data, plans, analysis reports, etc (see Figure 2 above on page 8). In theory, any of the CE VO's business partners (ConsEng, SP, HPC) could disclose confidential information to a third party. Any of the information designated by the rightholder as confidential, could be disclosed in

their entirety or in a subset. The disclosure could occur through negligence or on purpose. Moreover, a third party may intentionally get access to such sensitive information, through exploiting insufficient security mechanisms or could discover them by mistake.

The central legal vulnerability in relation to information designated as confidential is that its legal protection depends on its secrecy, or at most its limited accessibility[6]. Hence, if the information reaches the public domain and becomes common knowledge in the field through e.g. communication to the public, the stakeholder would lose its legal protection, although he would be left with possible claims for damage against those responsible for this loss. This risk scenario would directly affect the competitive advantage afforded by the confidential information, since arguably its market value is substantially reduced once the information is available in the public domain. The loss, and therefore the damages that could be awarded, would essentially depend on the initial value of the confidential information, the fraction of it being available in the public domain, and the degree to which competitors would be able to utilize the information for their own purposes (which may be limited if the publicly available information can not be utilized without additional understanding of other information which may still be confidential).

The likelihood of this risk scenario will, among other factors, depend on the level of control by the CE VO (see below 4.5) as well as the trustworthiness of the business partners and the level of security offered by the business architecture utilized for the collaboration.

4.3 Risk 2: TC ConsEng utilizes confidential information for competing purposes

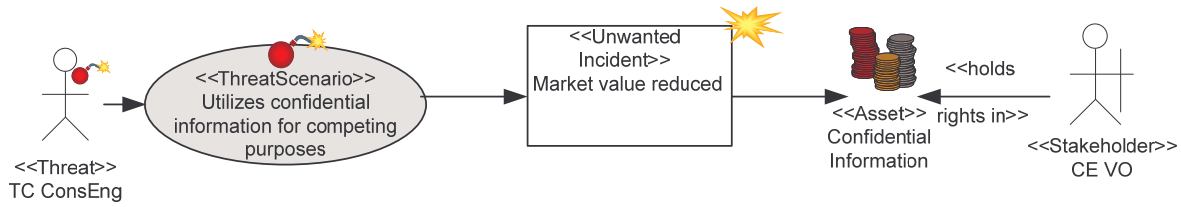

Figure 4 Utilization for competing purposes

The second risk relates to the possibility that any of the business partners utilizes the confidential information for competing purposes. In practice it is questionable whether the storage provider or the high-performance computing service would have any interest in utilizing the confidential information. Most likely, they would not have any use for airplane design data unless they closely collaborate with any of the competitors of the CE VO (see below 4.4). The existing business relationships

[6] refer to section 3.1 and 4 of the Legal Analysis of confidentiality

of the CE VO's partners in the scenario would hence be a factor that may have influence on the risk level.

With respect to the ConsEng, the situation seems to be somewhat different. If we assume the consultancy has a special expertise with respect to aerospace engineering, they would indeed have use for design data, which could be relevant for future consultancy for other companies. Hence, the possibility of the ConsEng utilizing confidential information for competing purposes can not be completely ignored. If this happened, it could at least potentially reduce the competitive advantage of the CE VO with respect to the improved airplane design, thus affecting the market value of the confidential information for the CE VO.

4.4 Risk 3: Confidential information utilized by competitor

The third risk relates to the possibility of confidential information being disclosed to a third party and subsequently being misused by a competitor. This risk scenario combines elements of the above mentioned two risks, since it involves the disclosure of confidential information to a third party (like in risk 1) and the utilization of confidential information for competing purposes (as in risk 2). This risk may only materialize if we assume a combination of disclosure to a third party (who may not be a competitor), a possible subsequent disclosure to a competitor and the utilization of the confidential information by the competitor. This would again affect the market value of the confidential information for the stakeholder, as this may reduce the competitive advantage of the CE VO based on the confidential information. However, this would only apply if the airplane plans, design data, analysis report etc. would be utilizable by a competitor, e.g. if the suggested solution may be applied in a similar way to other aircrafts or if the data indicates that a particular design is not feasible, and should therefore not be chosen by the competitor. This risk scenario is illustrated below in Figure 5.

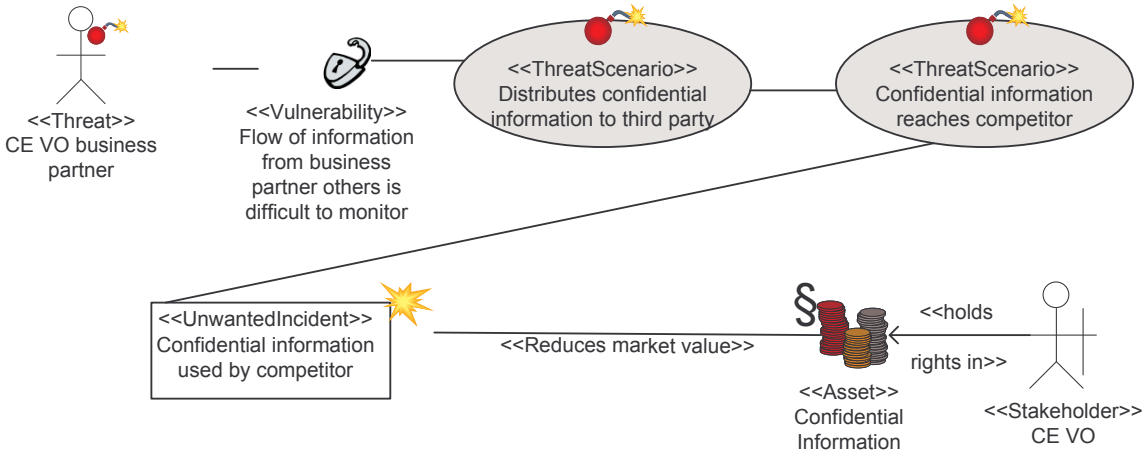

Figure 5 Confidential information utilized by competitor

4.5 Risk estimation based on level of control in different business models

The risk value for the above mentioned risks may to a certain degree depend on the business model chosen for the collaboration. The risk level will moreover depend on the quality and trustworthiness of the contractors. The risk level may thus be influenced by utilizing trust and reputation management as well as a suitable supplier selection mechanism (see for details TrustCom Deliverables D 59, Sections 3 and 4).

Three business models for the CE scenario, which are analyzed in more detail in D 59, are depicted in Figure 6.

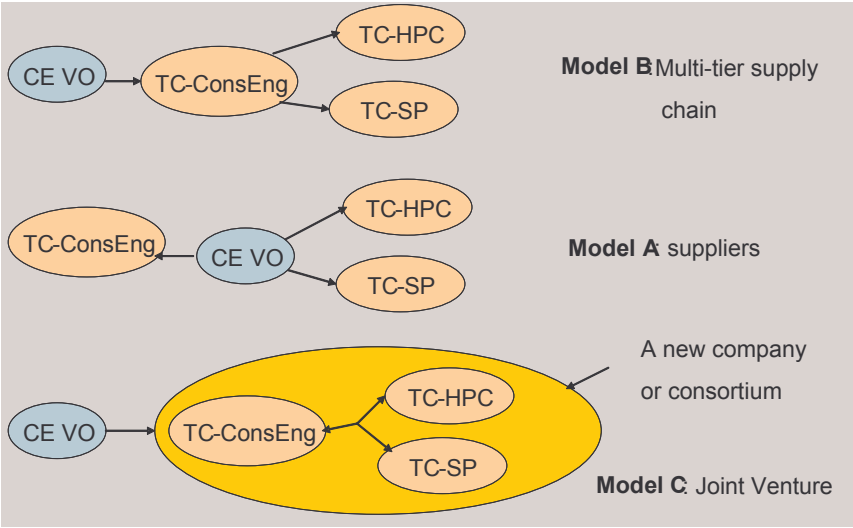

Figure 6 Business models (from WP 8, D. 59)

These business models differ essentially with respect to the level of control they allow the CE.

In model A, the CE VO maintains direct contractual relationships with all other involved actors, which thus are directly bound to the conditions agreed with the CE VO. This model implies arguably the highest coordination costs for the CE VO, but on the other side it affords maximum control.

Model B is the classical sub-contracting model, where the CE VO subcontracts with the consultancy company Cons-Eng, which again establishes and maintains contracts with TC-HPC and TC-SP. This model transfers some of the management and coordination to TC-ConsEng, but may contribute to a reduction in control of the subcontractors. The amount of control will essentially also depend upon the constraints imposed on TC-ConsEng with respect to subcontracting, e.g. whether TC-ConsEng may freely choose subcontractors, whether the subcontracting organizations and their employees will be subject to specific non-disclosure agreements, etc.

Model C contains is based on a collaboration between TC-ConsEng, TC-SP and TC HPC, which then together have contractual relations with the CE VO. The level of control may to a certain degree depend on whether the collaboration between the three organizations is of a mere contractual type, or whether a new business entity with legal personality is established.

The analysis of the alternative business models indicates differences with respect to the level of control of the cooperation. Arguably we may assume that the risk from the perspective of the CE VO will be reduced with an increase of control of the contract partners.

Depending on the selected business model, it will be possible to have different confidentiality arrangements:

While model A (suppliers) affords the CE-VO the highest degree of control, it also creates for it a need to enter into confidentiality agreements with each of these suppliers and monitor in each case the manner in which the contractual obligations assumed by the partners are respected. Since the nature of the business relation is different with regard to each of the suppliers (a consultancy contract with TC-ConsEng, a service provision contract with TC-SP and another one with TC-HPC), the nature of the confidential information exchanged and more importantly, the specified purposes allowed under the confidentiality agreement differ. Moreover, since these partners handle (access and use) confidential information at different moments in time, the duration of their obligations differs as well. That makes it highly unlikely that one single standard-form and all inclusive confidentiality agreement could be envisaged for all of these business relations.

On the other hand, since the CE-VO enters into separate agreements with nominated business partners, the contract specifications in this model risk being flawed regarding of the non-functional requirements identified in Section 6.2 of this Annex, that is supportability, since the agreements will be difficult to amend despite changes in circumstances (such as the identity of one of the VO members).

Model B is seems to be more flexible than the previous model. It allows the CE – VO to transfer in the hands of his main contractual partner, TC-ConsEng, the contractual risks as well as the responsibility for the attainment of specified security standards by the second tier suppliers. As explained in detail in Section 5.1.3.3 of the main report, it is possible for CE-VO and TC-ConsEng to agree on certain confidentiality policies involving all confidential information to be exchanged throughout the collaboration, regardless the identity of the involved VO members at a certain point in the collaboration. TC-ConsEng will have the possibility to impose this standard on the second tier suppliers as a precondition for collaboration. However, in case the second-tier suppliers do not respect the compulsory standards of confidentiality or the imposed access procedures, the CE-VO will be able to enforce the contract only against the TC-ConsEng, a solution that may in practice prove slow and with limited use[7]. Considering the confidentiality

[7] By this I mean that it will be possible to ask for damages for the prejudice suffered, but the prejudice will have already occurred.

arrangements, this business model has therefore a minus in terms of reliability and performance.

According to Model C, TC-ConsEng, TC-SP and TC-HPC have together contractual relations with the CE-VO. This model facilitates a more all-inclusive model if confidentiality agreement, especially in terms of those common provisions that are likely to appear in such an agreement (for example the information that is to be designated as confidential, the symbols that are supposed to make it identifiable as such, the duration of protection, the procedures involved in the destruction or the return of the documents once the tasks are completed). This would represent a plus in reliability and enforceability (since the responsible partner, directly designated as part of the confidentiality agreement, can be held accountable more rapidly).

It is worth mentioning again that business entities will enter one or more confidentiality agreements only when pre-existing or envisaged business relations or collaborations would necessitate a safe disclosure of sensitive information. Otherwise confidential information is kept secret and exploited only by its right holder.

5 Treatments

The following section presents treatment options for the risks identified above.

5.1 Treatments to Risk 1

The first risk described above relates to the confidential information being disclosed to a third party, reaching the public domain and losing its legal protection. As mentioned above, the value of this risk (a function of its likelihood and its consequences), will depend both on the trustworthiness of the CE VO's partners, the level of control the CE VO has over its business partners, the security of the architecture utilized for the collaboration and the value of the confidential information for the stakeholder CE VO. Consequently, the treatments for this risk will have to target the risk value, either by reducing the consequence value, or by reducing the likelihood of the unwanted incident. The consequence value will essentially depend on the value of the confidential information, or part thereof, which loses its legal protection. Hence, the possibility of controlling the consequence value would essentially imply that the CE VO seeks to reduce the amount of confidential information being communicated (access to confidential information on a need to know basis), see below Figure 7.

Role	Access Rights to PDD
Structural Designer	Structures data: aircraft surfaces and internal structural data
EM Designer	Avionics: comms and control system data
EM Analyst	Avionics + aircraft surfaces only
CFD Analyst	Aircraft surfaces data only

Table 1 Example of role-based access control

This appears to imply a possible conflict with the aim of the collaboration of the scenario, i.e. the effective and efficient design of the upgraded aircraft. Following a cost-benefit analysis, the reduction of access to confidential information would thus need to imply that access is provided on a need to know basis. An example of a role-based approach to control is illustrated in Table 1.

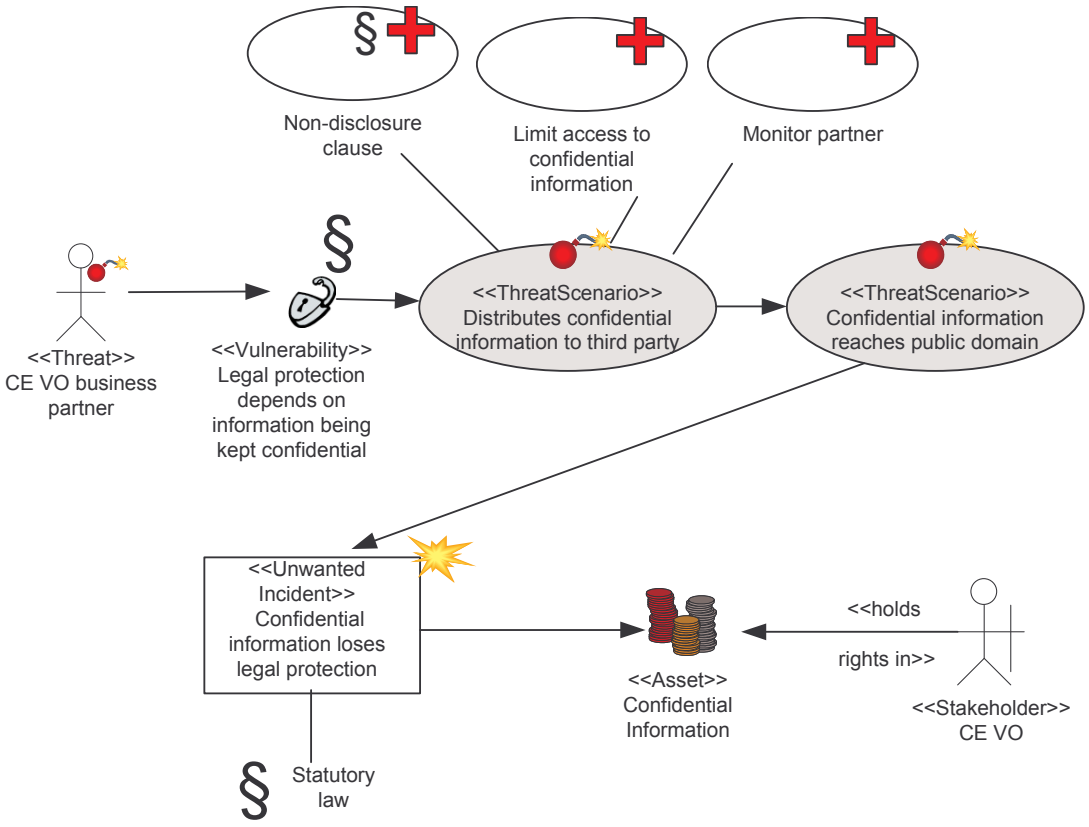

Figure 7 Treatments to prevent loss of legal protection

The second treatment strategy included in Figure 7 involves the reduction of the likelihood of the unwanted incident. In order to achieve this, one would have to strengthen the control of the flow of confidential information in the scenario. This can be done either by legal means, i.e. introducing a non-disclosure clause in the contract, as well as by improving the security of the technical architecture and of the business processes. Moreover, some reduction of the likelihood of this risk may be achieved by introducing a monitoring procedure, which allows the CE VO (or a trusted third party) to monitor data flow in order to prevent, identify and adequately address the unjustified flow of confidential information.

Hence, the strategy to reduce this risk would imply a combination of technical measures, business processes and legal means.

5.2 Treatments to Risk 2

Risk 2 implies the utilization of confidential information by a contract partner for competing purposes. As mentioned above, the partner most likely to have an interest in the utilization of confidential information for competing purposes would be the ConsEng. A treatment strategy would again involve measures to reduce the

consequences of this unwanted incident as well as measures to reduce its likelihood. The consequence-reducing measures (in particular access on a need to know basis) were already addressed in the previous section.

With respect to the likelihood of the threat scenario, the task is to identify measures that will effectively prevent ConsEng from a competitive use of the confidential information. The treatment strategy will again comprise legal as well as business process-related and technical measures. With respect to the required legal agreement, the essential contractual provision would stipulate a limitation of the use of confidential information to the project agreed between the CE VO and its business partners. This clause would of course need to be interpreted in the specific context of the scenario, in order to delimit which use can be deemed to be project-related.

In addition, the effectiveness of this clause could be ensured by an obligation to delete data after having finalized the analysis and by putting in place a suitable monitoring process, which allows a subsequent audit. The objective of this monitoring and auditing process would be to prevent, identify and address the utilization of confidential information for non-project-related purposes.

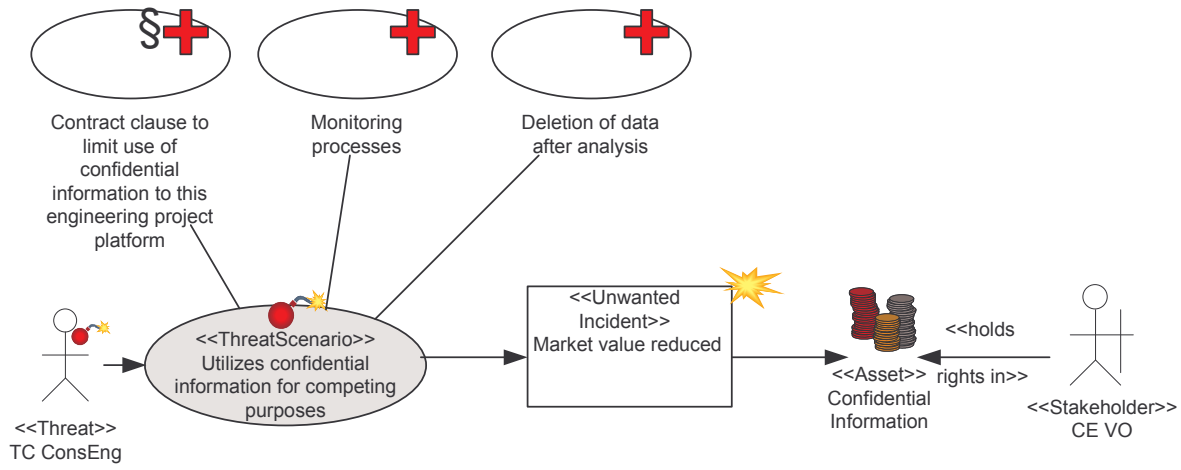

Figure 8 Treatments potentially reducing utilization of confidential information for competing purposes

5.3 Treatments to Risk 3

Risk 3 covers the disclosure of confidential information to a third party, eventually reaching a competitor and being misused for competing purposes by the latter organisation.

The treatments to this risk are similar to Risk 1. A non-disclosure clause in the contract should prohibit the disclosure of confidential information to third parties. However, the challenge is to balance this non-disclosure obligation with a

permission to disclose confidential information to the other organisations involved in the collaboration, in order to ensure the smoothness of the business processes. The non-disclosure obligation would thus not be unlimited; it should to take into account the need to communicate confidential information and the permission to disclose confidential information to those partners that need it in order to fulfil their tasks and obligations.

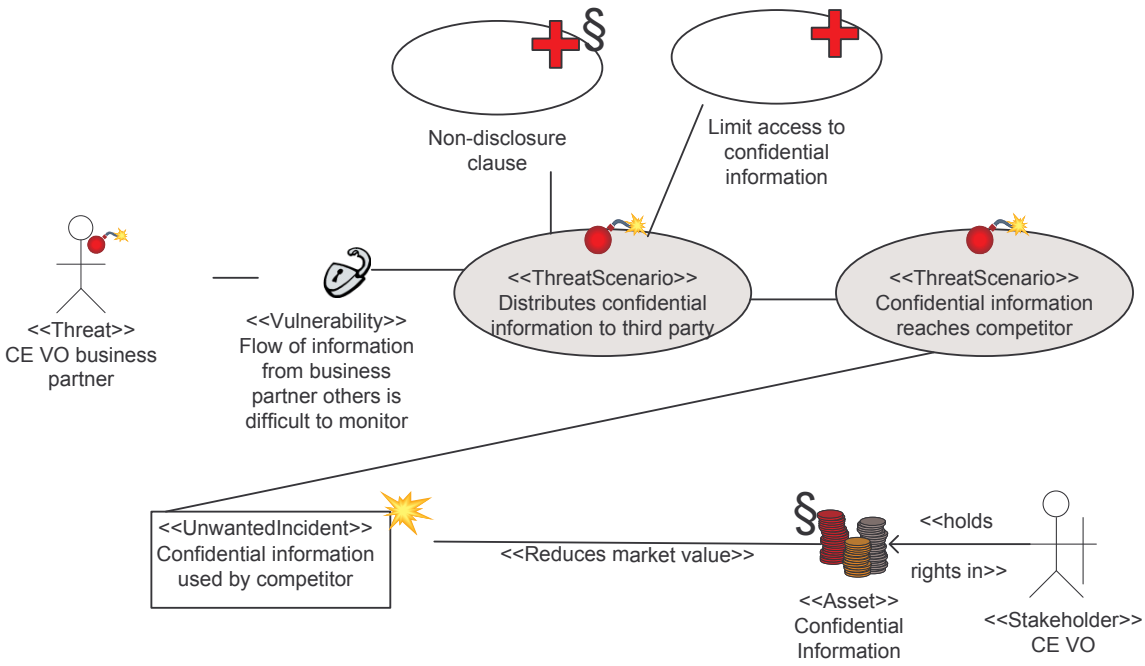

Figure 9 Treatments to prevent confidential information reaching third party

5.4 Treatment overview

The following Table 2 contains an overview of the identified risks and the relevant treatment options, concentrating on the non-disclosure clause in the respective contracts. The inclusion of the risk as well as its risk value and treatment measure in one table should allow some degree of traceability. Thus, the collaborators will be able to identify why a particular contract clause is suggested and they should be able to analyze whether the suggested treatment measure effectively reduces the value of the risk.

	Con-sequence	Likelihood	Risk value	Treatment
Risk 1 **Distribution -> loss legal protection**	Major	Possible	Major	Avoid distribution to public through confidentiality clause
Risk 2 **Utilized by TC ConsEng for competing purposes**	Major	Possible	Major	Limit use to project related purposes
Risk 3 **Utilized by competitor**	Major	Possible	Major	Avoid distribution to competitor: confidentiality clause

Table 2 Risk and treatment table

6 Contract requirements based on a cost-benefit analysis of treatments

As mentioned above in Section 3.3, the contract requirements may be defined as a list of functional, non-functional and external requirements. The contract requirements should be identified based on the risk and treatment identification described above.

6.1 Functional requirements

The functional requirements describe the functions of a contract. This should include both the achievement of a goal and the management of risks that are inherent in the situation addressed by the contract.

The primary goal of the contract between the CE VO and the other organisations would be to allow the collaborators to communicate efficiently in order to enact the agreed business processes and to fulfil the objective of the collaboration, i.e. to analyse the design of the improved airplane. The intended communication and interaction between the participants is illustrated in Figure 2.

Moreover, the functional requirements of the contract should ensure the management of the risks related to the collaboration, in particular with respect to confidentiality. The functions of the confidential agreements incorporating the type of clauses proposed in Section 5 of the main report is to protect confidential information and to ensure secure and trusted communication flows among the VO partners and between them and other members of the business environment. Furthermore, it should enable the management of risks inherent to the disclosure of confidential information in a collaborative engineering environment on the Internet in which the automation and flexibility of the business processes are basic features.

However, the requirements have to be analysed in connection with their potential costs. This requires the performance of a cost-benefit-analysis of the suggested requirements, to determine whether the proposed measure will have the expected effect on the risk value and in order to assess whether the costs generated by the proposed measure are justified by the measure's effects.

In order to manage the risks related to confidential information, the contract would have to define what is to be understood as confidential information and how it is to be identified (Risks 1-3). Moreover, the risks 1+2 (disclosure) and risk 3 (misuse of confidential information by collaborator) would need to be managed as follows:

In order to manage risks 1 and 2 (disclosure), the suggested treatment option is to prohibit the disclosure of confidential information to third parties. A cost-benefit analysis of this proposed measure indicates the following: The cost of including this clause could initially be deemed to be rather low, since this is a standard procedure in commercial contracts. One might however argue that the fulfilment of this obligation could be rather costly, as collaborators would have to spend substantial effort on managing the data flow in order to avoid a contract breach. Thus, if the

costs of fulfilling this obligation are taken into account, the costs of this measure could be said to be at medium level. The likely benefits of this contract clause are on the other hand difficult to determine. It is not clear whether such a prohibition actually would inhibit a contractor from disclosing confidential information, if the profit from disclosure exceeds all possible negative consequences of disclosure. However, we would have to assume that this obligation would have a high importance for most organisations, and that this measure thus would imply a substantial contribution to preventing disclosure. In conclusion, the benefits of including a non-disclosure clause would most likely largely exceed the costs of including it in the contract.

With respect to Risk 3 (misuse of confidential information by contractor) the suggested treatment measure was to contractually limit the use of confidential information to project-related purposes, by prohibiting utilisation of confidential information for non-project-related purposes. The cost-benefit analysis of this measure seems to be parallel with the previous. The cost of including the clause in the contract would in itself not be very high, but the monitoring of the fulfilment of this obligation could generate considerable costs for all contractors. The benefit of the suggested clause is difficult to anticipate. It seems however reasonable to assume that most contractors would consider this clause when utilizing the confidential information, and that the likelihood of contractors utilizing confidential information for competing purposes would be somewhat reduced.

However, the benefit of these prohibitions would essentially also depend on whether these are combined with other approaches (in particular technical architecture and business processes), and whether there are mechanisms to ensure the effectiveness of the contract obligations. The effectiveness of the contractual obligations would thus depend on sanctions available in the contract or in the governing law, on liability and liability caps, etc. Moreover, the effectiveness of the contractual obligations would also depend on the degree to which the stakeholder of the confidential information is able to monitor the interactions, and whether the contract partners expect that such monitoring will reveal contract breaches.

Summing up, we can conclude that the functional contractual requirements should include measures to ensure the functioning and efficient communication between the partners, as well as the management of the identified risks to the confidential information through the contract clauses mentioned above (which will be discussed in more detail in Appendix B, in combination with a number of other measures.

6.2 Non-functional requirements

In addition to the functional risks, there will be a number of non-functional risks as described above in Section 3.3, which will need to be taken into account when drafting the contract.

If they are to be a suitable tool in managing the access to confidential information in the TrustCom framework, the confidentiality agreements entered into by the VO partners need to be usable, reliable, to facilitate the performance and be manageable (that is satisfy the supportability requirement). Moreover, parameters

regarding the contract validity or enforceability should be commonly agreed. In the following we will exemplify how contractual clauses as those explained in Section 5 of the main part of this Deliverable can contribute to the fulfillment of the non-functional requirements to a contract.

- Usability

The confidentiality agreement can be made more accessible to non-lawyers as long as the parties themselves negotiate its terms and participate in the designation of confidential information. The list of information that is to be treated as confidential and the security standards to be complied with, as well as the duration of the contractual obligations (highly dependant on the usefulness of the information) or the consequences of illegal disclosure would arguably be better understood and assessed by non-lawyers. This information is dependant on the commercial practices in a given field of activity, internal policies and the concrete conditions of the business environment, therefore more available to the practitioners then to their legal advisors. Once these basic clauses have been negotiated, their automation is made possible by the various clear parameters included in their provisions (authorized or not, protected or not, in effect or non applicable anymore).

- Reliability

As explained in Section 5 of the main report, there are several ways to increase the certainty of the rights guaranteed by the parties, including but not limited to the conventional designation of the information to be provided, of the duration of the obligations, the specified uses, the security standards to be complied with or the amount of money to be paid in case the rights of the disclosing party are not respected. As long as these parameters are commonly agreed by the parties, there are increased chances that the agreement is more reliable.

- Performance

Even though it is important to include procedures in the contract which can contribute to the effective protection of confidential information, parties need to ensure that these processes must work in practice and are not excessively time-consuming. This means that the processes required for the treatment of confidential information should not be excessively bureaucratic. Arguably, this can be achieved by having in mind why the contract clause is being introduced (risk identification), and by assessing the cost-benefit relation between the contract clause/procedure in question and the respective improvement of the protection of confidential information. Moreover, parties may need to consider the risk that too complicated procedures may not be followed in practice unless compliance is monitored and enforced.

- Supportability

The parties could for example agree mutually on the modification of the contractual terms. At the same time, the ease with which changes in circumstances are reflected into amendments of contractual clauses is dependant more on the flexibility of the main contractual arrangements than on the provisions of the confidentiality agreements. Even so, as explained in Section 5.2.1 of the main report, the contractual obligation of confidentiality can survive even after the main

collaboration between parties ended, which is likely to decrease the likelihood of misuse of the information due to abrupt change in the VO membership base.

External requirements

Moreover, there are some external requirements for the relation between the contract and its legal context. In particular, it will be a requirement that the contract is *valid.* The rules for the validity of contracts will need to be taken from the governing law. However, in general, there will be some formal requirements to the contract (for certain contracts, a particular form is indispensable) and there may be material requirements (e.g. relating for example to the quality of consent given by the parties when entering the contract).

Secondly, it will normally be a requirement that the contract should be *enforceable*, and procedural as well as material norms may have an effect on the enforceability. In some cases, clauses will be included in a contract despite there being a doubt whether this may invalidate the contract or inhibit its enforcement. In this case, contractors may assume that the other party will not test the enforceability in a formal procedure, but rather follow what was contractually agreed, despite the lacking enforceability of the contract clause. Another solution might be that the parties expressly state that the clauses of the agreement are severable, which as explained in Section 5.1.4.2 will decrease the likelihood of the whole agreement being invalidated due to the nullity of one single contractual clause.

7 Contract drafting – example clauses

Subsequent to the identification of contract requirements, the stakeholder will want to draft a contract that complies with the identified requirements. The following exemplify confidentiality clauses that could be inserted by the CE VO in its contracts with its competitors. [8] For more detailed clauses, reference should be made to Appendix B of the Study.

Example 1: General clause, designation procedure and obligations

- The Members shall treat as confidential any information that a disclosing Member has designated as such.

Designation as confidential

- A disclosing Member shall designate information as confidential at the time of disclosure either (1) in writing, such as by a stamp, legend or cover letter, or (2) orally, so long as the confidential nature of the information is then confirmed in writing as above within fourteen (14) days of the disclosure.
- A designation of confidentiality shall be of no effect if, at the time of the disclosure or designation (whichever comes first), the information was:
  (a) Already published or otherwise available to the public; or
  (b) Already in possession of the receiving Member.
- A designation of confidentiality shall be of no effect if, after the disclosure or designation, the information is:
  (a) Published or otherwise made available to the public by the disclosing Member or by a third party through no fault (i.e., act or omission) of a receiving Member;
  (b) Obtained independently by the receiving Member from a third party and without any breach of a secrecy obligation; or
  (c) Developed by or for the receiving Member independently of the confidential information received from the disclosing Member.
  - A designation of confidentiality also shall be of no effect insofar as the information so designated must be disclosed to comply with applicable laws or regulations or with a court or administrative order, provided that the receiving Member shall inform the disclosing Member of such a requirement and continue to otherwise perform the confidentiality obligations contained in this Agreement.

Obligations

- A receiving Member shall not:
  (a) Use any confidential information for any purpose other than in accordance with this Agreement or a Project Agreement;

[8] Cf. confidentiality clauses in Legal-IST report "Report on Legal Issues in SME clusters", www.legal-ist.org.

(b) Copy or otherwise reproduce any confidential information, either in whole or in part, unless such copying or reproduction has been authorised in writing by the disclosing Member; or
(c) Disclose any confidential information to any third party (other than employees of the receiving Member) unless authorised in writing by the disclosing Member.

Employees

- The Members shall contractually impose the same obligations on all of their employees who may have access to confidential information, to the maximum extent and for the maximum duration authorised by law, including upon the end or the termination of their employment.

Example 2: Alternative single confidentiality clause[9]:

Confidential Information means all information (oral, written or in electronic form) obtained by one party from the other pursuant to this Agreement which is expressly marked as confidential or which is confirmed in writing to be confidential within *7* days of its disclosure.

Each party shall treat as confidential all Confidential Information and shall not divulge such Confidential Information to any person (except to such party's own employees and then only to those employees who need to know the same) without the other party's prior written consent provided that this clause shall not extend to information which was rightfully in the possession of such party prior to the commencement of the negotiations leading to this Agreement, which is already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this clause) or which is trivial or obvious. Each party shall ensure that its employees are aware of and comply with the provisions of this clause. If the Supplier shall appoint any subcontractor then the Supplier may disclose Confidential Information to such subcontractor subject to such subcontractor giving the Customer an undertaking in similar terms to the provisions of this clause, and the Supplier shall in any event be responsible for any breach of the obligations of confidentiality contained in this clause by such subcontractor. The foregoing obligations as to confidentiality shall survive any termination of this Agreement.

[9] Morgan and Burden on Computer Contracts. 7th edition, London 2005, p. 349.

8 Risk checklist

Based on the findings of the legal analysis in the main report and the legal risk analysis of the CE scenario in this Appendix, we have summarized our findings in a risk checklist, which provides examples from the scenario.

Several confidentiality risks may materialize in the TrustCom CE scenario since the VO members have various informational assets. As illustrated by Figure 1, their collaboration is dependant either on exchange of such information or at least on access to the confidential information of others.

As described in Section 3.1 of this Appendix, the typical risks to confidential information can be identified based on a suitable checklist including specific legal risks and risks that may arise from the configuration and the specifications of the VO collaboration and that have legal treatments. The risk treatments for each of the identified risks will be formulated as contractual requirements within Confidentiality (non-disclosure) agreements[10]. The chosen risk treatments will reduce either the likelihood of the risk or its consequences.

This following checklist will only address risks for which there is a legal treatment available, although other risks of a more technical nature and with technical treatments may be equally relevant. Such other risks – which are omitted here – may pertain for example to:

- access policies being incompatible due to different understanding of "confidentiality";
- access tokens not granted due to insufficient documentation of the "need to know"
- delayed activation of access policies due to uncertainties regarding the status of certain information : prior knowledge- recent acquisition following the disclosure.

The following are risks that result from general (contractual) or specific (pertaining to the legal protection of the undisclosed information) legal rules or principles regarding the access and use of information designated as confidential.

8.1 Definition and scope of "confidential information"

In TrustCom, the collaboration is modeled as a Virtual Organization involving virtualized services and roles that could be hosted in arbitrary domains and which is subject to policies defined at a high level within the collaboration[11]. Not only does this require a flexible and adaptative membership management, but it also opens

[10] For reasons as those presented in Section 4.1 of the main report, we do not recommend that confidentiality issues are addressed as one clause within the main collaboration agreement between parties, but rather more thoroughly in a separate document (confidentiality agreement).

[11] See TrustCoM Deliverable D 10, Baseline prototype infrastructure for the CE Scenario

up the challenge of synchronizing different legal backgrounds if partners are located in different European countries.

As explained in Section 3.1 of this study, neither the definition nor the scope (the kinds of information that could be protected by confidentiality) of "confidential information" is similar in all the European countries. This situation increases the risk that the VO members will design their access policies around the protection of different types of information and consequently will exclude from the scope of protection others, possible more sensitive from other partner's point of view.

Legal treatment: A contractual clause clearly defining what information will be protected as confidential and how future information or documents deserving protection will be marked.

Effect: Decreases the likelihood of confusion as to the access policies to be applied with regard to a given information.

8.2 Negative know-how

Negative "know-how", that is the information regarding failures in production processes, incomplete or erroneous data, irrelevant or unfavorable factors may prove an important asset both for the CE-VO and the TC-ConsEng, since this knowledge prevents unnecessary duplication of research, analysis and development efforts and enables efficient allocation and management of financial and computational resources during the VO lifecycle. The confidential information (input or output data) exchanges among the VO partners are highly dynamic and influenced by the results of the simulations and conclusions of the analysis reports performed The legislation leaves it up to the parties to protect it as confidential or not.

Legal treatment: Express contractual clause stating each VO members' option in protecting as confidential negative know-how.

Effect: Decreases the likelihood of unclear access and use policies or inadequate tokens for access to negative know-how.

8.3 Prior knowledge

As explained in Section 3.1.1 of the main part of this Deliverable, information can be legally protected as confidential even if it is not unique, in the sense that other businesses that came to its knowledge through lawful means may chose to keep it secret too and agree to disclose it under the restrictive terms of confidentiality. This situation is particularly relevant for the TC-ConsEng, that due to its vast consultancy and analysis expertise it is very likely to have already gained knowledge of facts and data that his contractual partner, for example CE-VO or TC-HPC wishes to have protected by confidentiality. From the TC-ConsEng perspective, that would equal to unnecessary constraints and limitations regarding its ability to use the result of its own research in the most business lucrative way.

Legal treatment: Contractual designation of circumstances in which confidentiality obligations do not exist irrespective of the content of the information exchanged. Such circumstances may refer to:

- prior knowledge
- information already in the public domain
- information required to be disclosed by law or legal action
- independently developed by employees or affiliated companies of the receiving party without any knowledge of the disclosure that is about to be made.

Effect: Attenuates the consequences of over-reaching contractual constrains. On the other hand, it may be technically difficult to distinguish between prior knowledge and knowledge acquired as a result of the disclosure. This risk cannot be mitigated through contractual means, but it will have to be tackled through technical means.

8.4 Negotiations with potential VO members

The temporary expansion of the CE VO with an additional engineering design consultancy ("TC-ConsEng") and providers of IT services that support the design and analysis process as a result of the newly arisen business opportunity will involve negotiations between the prospective partners. During the negotiations, the CE-VO members need to disclose certain information relevant in assessing the others' availability, competence, expertise in fulfilling the collaboration objectives. Since at this point the outcome of negotiations is uncertain (it is uncertain if the parties will become contractual partners), the risks of disclosure of confidential information are high.

Legal treatment: Parties should agree at this early stage (during negotiations) on the procedures involving each other's confidential information.

Effect: Decreases the likelihood of disclosure of the VO member's confidential information by prospective VO partners.

8.5 Unlawful disclosure by VO members

The fact that the VO members agreed on certain confidentiality policies, implemented security measures and the access to confidential information is based on tokens agreed by the partners does not mean that those employees of the VO members that do have a need to know and the right to have access to confidential information will not act in bad faith by unlawfully disclosing it to third parties. Hence, there is a risk of unlawful disclosure or use by VO members who have legitimate access to the information.

Legal treatment: Restrict access on a need to know basis and have the employees of the VO members with access rights sign confidentiality agreements.

Effect: Attenuates the consequences (financial damage caused by confidentiality loss) of the unlawful disclosure. Even though it does not hinder bad faith behavior, it provides the legal basis for a request for damages in accordance with the loss.

8.6 Unlawful disclosure by external third parties

This risk (third party intrusion) could be regarded as intrinsic to any security system aimed to protect sensitive information. Even though in this case the provisions of a confidentiality agreement are not applicable[12] the law (criminal law more precisely) may be the only solution where the security system failed.

Legal treatment: Stipulate in the main collaboration agreement the obligation to monitor and be able to document those elements that are constituent of a crime (according to criminal law) (such as: the malicious intent, the source of the intrusion, the exact information asset that was misappropriated, or the consequences of the intrusion)

Effect: Decrease the consequences of the risk through facilitating the identification of the intruder with the view of claiming back the financial loss occurred due to the offence.

8.7 Confidential information is lawfully discovered by a third party and made public

Due to the specific conditions stipulated by the TRIPs Agreement[13] and the associated national laws implementing it, legal protection is afforded to confidential information provided it remains secret to the general public.

If one or more of the VO partners' sensitive information protected by confidentiality agreements and proper security systems becomes common knowledge in a manner that is not "contrary to honest commercial practices", the legal protection and the market benefit is lost without any possibility to claim damages. This would include reverse engineering, independent research etc.

Legal treatment: The VO members should explore the possibility of protecting sensitive, valuable business information through more proprietary means of protection of intellectual creation (such as patents and copyrights).

Effect: Decreases the level of the financial loss caused by inadequate legal protection of sensitive, undisclosed information.

8.8 Confidential information misused by VO partner

The disclosure of confidential information occurs from one VO member to another for specified purposes. For example, TC-ConsEng will retrieve the design model data in the context of a simulation or 'job' stored by the CE-VO in the location provided by the storage provider for the model input data; TC-HPC, the provider of HPC-based application services will have access to the analysis report done by the TC-ConsEng; The processes that are part of the communicational workflow place

[12] see Section 4.3 of the main report for details

[13] see Section 3 of the main report for details

different constraints (in terms of security access policies, required SLA) on the behaviour of the VO members that perform the role of "authorised person". The trust-based security framework ensures that operatives with the role 'Analyst' in TC-ConsEng are able to access the HPC service and the storage provider services with appropriate trust credentials that are acceptable to the partners[14]. However, the likelihood of bad faith misuse of the confidential information to which access is granted is high among the authorised personnel, since the appropriate tokens exist already for these roles.

Legal treatment: Stipulate expressly in the confidentiality agreement the authorized/ non authorized uses (what is the purpose of the disclosure)

Effect: Although it does not impede acting in bad faith, it decreases the likelihood of accidental misuse (through an extensive personal interpretation of the work duties) and provides a sound legal basis for damage claims or for injunctions to stop the unwanted behavior.

8.9 Negligence

The confidentiality relation is a relation of trust between the entity disclosing the information and the receiver. This relation extends beyond the common business interest, as it is tightly connected linked with the belief that once disclosed, the information will be protected by the receiver to the best of his ability, in good faith, not only against misuse by employees but also against third party intrusion. There is a risk, however, especially in the multi-tier supply chain contractual model, that the CE-VO will not be in control of all the Policy, Trust and Security components implemented by the tier-n suppliers, and will have limited practical ability to control the selection of trustworthy partners.

Legal treatment: Insert in the confidentiality agreements an express clause to take certain specified measures to hinder unauthorized access to the information entrusted by the other. Such measures could be both contractual and technical, and not complying with them would equal contractual infringement.

- to ensure the same standard of protection for the confidential information received from the contractual partner as for his own confidential information
- to impose confidentiality obligations on the employees of the receiver
- to keep the confidential information from different business partners in different locations
- to notify when a confidentiality breach has occurred and to disclose the identity of the infringing party

Effect: Decreases the likelihood of negligent handling of confidential information which would result in accidental or indirect disclosure of confidential information and facilitates the burden of proof in case an infringement occurred.

[14] see TrustCom Deliverable D41

8.10 Misuse after the fulfilment of tasks

This risk is especially relevant for the temporary roles designated during the operational phase of the VO lifecycle. For example, the lifetime of the "mini-VO", Job-VO[15] supporting the analysis work in his company, TC-ConsEng is coupled with the contract of TC-ConsEng with the CE VO: when this terminates, the Job VO is dissolved. However, the Job-VO gained access to confidential information as part of completing the tasks it received. There is a risk that confidential information is stored elsewhere (intentionally or de facto) and misused once the tasks are fulfilled and the obligations towards the TC- ConsEng and CE-VO.

Legal treatment: The parties should have the obligation to return to their legitimate owner or to destroy the documents referring to the confidential information upon completion of tasks.

Effect: This legal treatment will decrease the likelihood of misuse of "residual" confidential information. For additional guarantees, the VO members could agree on notifying each other when the documents were destroyed.

8.11 Application for patents or claim of other IP rights

The business collaboration within the CE-VO will result[16] in the upgrading of an aircraft fleet in order to support Internet access in the passenger cabin. This would involve installing new antenna and communications systems into existing aircraft. Since the collaboration involves confidential and proprietary information exchanges between the VO members, we can foresee a situation in which one of the VO members decides to file in an application for patents or claims other IP rights (for example decides to copyright a computer program or a database to which he gained access, or claims prior rights resulting from use) with regard to prototypes that are still under the temporary protection of confidentiality.

Legal treatment: Insert a "no implied license clause" in the confidentiality agreement. This clause reserves for the rightful holder all rights to the disclosed information, in particular the right to apply for patents and other protective rights. The receiver has therefore only the right to temporarily use it for specified purposes and cannot profit from the use of that knowledge outside the terms of the confidentiality agreement.

Effect: It reduces the likelihood of this risk occurring and moreover it clarifies the extent of the rights acquired by the receiver once he is granted access rights to confidential information.

[15] according to TrustCoM Deliverable D41, Enhanced prototype for the CE Scenario

[16] according to TrustCom Deliverable D10

8.12 Enforceability of confidentiality agreements

When one of the contractual parties culpably does not fulfill his obligations, the other party is suffering a loss. Therefore, invoking the rights he acquired via the agreement[17] he can demand that the other party fulfills the obligation assumed. If this proves impossible[18] the aggrieved party can demand and obtain damages for the prejudice caused by the other party through non fulfillment. In legal terms, this is called enforceability of contractual provisions. The possibility to enforce the contract against the person who doesn't fulfill his contractual duties provides the link between "theory" and "practice".

The main legal risk is that the nature and the extent of the prejudice suffered through non-fulfillment of contractual clauses needs to be proved, which may in itself prove as a cumbersome and time consuming task especially since the financial expression of a competitive advantage lost through disclosure of valuable confidential information is difficult to assess in practical terms.

Legal treatment: Insert a clause of "agreed payment for non performance". Thus, the rightful holder of information will be entitled to claim from the receiver the agreed sum of money whatever the extent of the actual prejudice he suffered.

Effect: Decreases the consequences of the confidentiality loss through guaranteeing to the aggrieved party a certain financial alleviation regardless of what he is able to document as loss suffered.

[17] for example the right to ask the destruction of the confidential information by the party to whom they were disclosed once the task is completed

[18] for example if the confidentiality protection is lost due to disclosure in the public domain