Risk Assessment of Security Critical Systems

Project Number:	IST-2000-25031
Project Title:	CORAS
Deliverable Security*:	RE
CEC Deliverable Number:	D7.4
Contractual Delivery Date:	31/12/2002
Actual Delivery Date:	24/02/03
Deliverable Title:	**Technology Implementation Plan, 1st Version**
Version:	03. 029. v01. WP7. Act. 7.6. D7.4
Principal WP Contributor:	WP7
Deliverable Type:**	R
Authors:	Demissie B. Aredo (editor)
Contributors:	Eirik M. Knudsen, Mass S. Lund, Siv H. Houmb, Katerina Papadaki, Ketil Stølen, Tony Price, Michael Loupis, Bjørn Axel Gran, Theo Dimitrakos, Atoosa P.J. Thunem, Gustav Dahl, Tony Price, Dimitris Raptis

*** Security:** PU – public. PP – restricted to other programme participants (inc. Commission Services).
RE – restricted to a group specified by the consortium (inc. Commission Services)
CO – confidential, only for members of the consortium (inc. Commission Services)

**** Type:** R – report. P – prototype. D – Demonstrator. O – other.

Abstract:	This document presents the Technical Implementation Plan (TIP) of the CORAS project, 24 months into the 30 month project. The TIP document describes the major results of the project, and how they will be used in practice.

Keywords:	Project results, dissemination, Community added value, market applications

Executive summary

This document presents the Technical Implementation Plan (TIP) of the CORAS project. The TIP document is intended to describe the major results of the project, and how they will be used in practice. The TIP document will evolve during the course of the project and goes through two main iterations. The first version of the TIP document is delivered at the end of month 24, whereas a revised version will be submitted at the end of project, i.e. June 2003.

This documents has three major parts. Part I provides a brief overview of the CORAS project objectives, anticipated results, etc. Part II describes the main results achieved in the project, whereas part III describes individual CORAS partners' plan for further collaboration in view of the implementation of the results.

The TIP is an internal document and its distribution is restricted to only the project partners and the project officer in the EU Commission.

1 Part I - Overview of the CORAS project and its results

a) Original research objectives

The CORAS project intends to develop a base framework applicable to security critical systems that will supply customisable, component-based road maps to aid the early discovery of security vulnerabilities, inconsistencies and redundancies. The CORAS main objectives are:

- To develop a practical framework for a precise, unambiguous and efficient risk analysis, by exploiting the synthesis of risk analysis methods with semiformal specification methods (in particular, methods for object-oriented modelling) and computerised tools, in order to improve the risk analysis of security-critical systems;
- To assess the applicability, usability and efficiency of the framework by extensive experimentation in the fields of e-commerce and telemedicine;
- To investigate the commercial viability of the CORAS framework and to pursue its exploitation within relevant market segments, while playing an influential role in standardisation organisations.

b) Expected deliverables

The administrative and research activities in the CORAS project and their results are documented and reported to the interested groups, i.e. partners, the EU commission, potential users, researchers, etc. in the form of deliverables. In addition to the contractual deliverables, results of the CORAS projects are disseminated to a wide range of audience through publications (papers, book chapters, invited presentations, etc.) The list of contractual project deliverables that provides information about major research activities, exploitable results, and contains the latest status of the technological development is included in Appendix A.

c) Project's actual outcome

The CORAS project is expected to achieve a particular solution for model-based risk management for security-critical systems. It also addresses issues related to the development environment for assisting the instantiations of the MBRM beyond the project period.

It will identify exploitation and dissemination directions of the overall concept (in terms of consultancy services) as well as individual exploitable components (methods, services or software) that can be standalone entities. The exploitation potential of the CORAS results mainly focuses on the health and e-commerce domains, for which the model-based risk assessment solutions are tailored. The concepts developed (in terms of architecture and methodologies) are expected to be very relevant to all security-critical systems, especially to telemedicine and e-commerce related applications. They are customisable and hence their potential is promising.

The main results of the CORAS project put the partners in a mutually complementary relationship. Commercial partner are fully convinced of the merits of the results that are achieved through their requirements and participation, and will integrate the resulting CORAS framework into their development process and introduce it into the industry. The research and development partners are working with standardisation bodies and major national institutions to exploit the CORAS results. They also put their efforts on necessary add-ons for enforcing policies at the administrative level through appropriate further tools. Finally, the educational partners are introducing the CORAS methodology into their curriculum.

d) Broad dissemination and use intentions for the expected outputs

The dissemination and use intentions of the CORAS results are derived as an extension of the respective roles of the partners in the consortium. The competences and interests of the partners in the CORAS consortium vary - from commercial partners to research and development partners to educational partners. The strength of CORAS is the combination of the different partners' competence; this reflects the work within the project duration and for fulfilling of the project's contractual requirements as well as all dissemination and use intentions after the project lifetime. Commitment to highly regulated risk management environment is also appropriate for major branches of the public sector including the e-commerce and telemedicine. For this reason, the CORAS consortium is well organised not only for exploitation, but also for dissemination and awareness creation of problems together with appropriate solutions.

To increase the dissemination and 'take up' of the CORAS results, a reference group consisting of expertise in the areas relevant to the project and from the industrial domain was established. The purpose of such an external reference group is to improve the quality of the CORAS results and widen the range of the dissemination of the results.

2 Overview of CORAS results

No.	Self-descriptive title of the result	Category A, B or C*	Partner(s) owning the result(s) (referring in particular to specific patents, copyrights, etc.) & involved in their further use
1	*CORAS Framework*	A	All partners
2	*CORAS methodology for Model-based Risk Assessment (MBRA)*	A	All partners
3	*UML profile for Security Assessment*	A	All partners
4	*Repository of Reusable Elements*	A	All partners
5	*CORAS Platform*	A	All partners
6	*XML format for representation of Risk Assessment*	A	All partners
7	*Vulnerability and Threat Management Component*	A	All partners

* A: results usable outside the consortium / B: results usable within the consortium / C: non usable results

3 Quantified Data on the dissemination and use of the project results

Items about the dissemination and use of the project results (consolidated numbers)	Currently achieved quantity	Estimated future* quantity
# of product innovations (commercial)		
# of process innovations (commercial)		
# of new services (commercial)		
# of new services (public)		
# of new methods (academic)		
# of scientific breakthrough		
# of technical standards to which this project has contributed		
# of EU regulations/directives to which this project has contributed		
# of international regulations to which this project has contributed		
# of PhDs generated by the project		
# of grantees/trainees including trans-national exchange of personnel		

*# = number of ... / * "Future" means expectations within the next 3 years following the end of the project*

3.1 Comment on European Interest

3.2 Community added value and contribution to EU policies

The modern community is in an ever-increasing manner relying on new and advanced services. In many cases, these services are of security critical character, and in order to reduce the vulnerability, extra care must be taken when implementing such services. The risks and the resulting vulnerabilities are frequently neither well understood nor analysed in any appropriate way.

Use of computerised systems for security critical purposes depends on trust in the systems. Trust is a subjective decision, which must be determined more or less independently by the actors involved. Increased knowledge of the risks related to the systems, and increased confidence that the security solutions that are implemented encounter these risks, are important parts of the foundation upon which trust can be built.

Data security is of prime importance in the information society world. As one example, commerce has always depended on the existence of a secure transportation network. This has always been one of the main functions (if not their proclaimed reason of existence) of organised states. The fact that communication network security has not been given full attention so far is expected to change soon, i.e., as soon as companies and organisations realise the full capabilities of data/telecommunications networks as transportation networks for (electronic) commerce.

A common source for problems may be differences or in the worst-case incompatibility between systems in different countries. For example, a telemedicine service may need to use resources in another country. It is therefore of main importance that the same levels of confidentiality and communication quality are supported in all the involved countries, because no chain is stronger than the weakest link. Very often there are different routines for handling sensitive information in different countries. Similar needs for co-ordination arise in areas like e-commerce and banking.

It may seem strange that modern states, which have a strong tradition in making and enforcing laws, which promote safety on their transportation networks and protect privacy and personal security, have done very little with respect to the information technology related aspects of these concepts. To meet these challenges the different countries must collaborate in order to agree on basic service attributes regarding different security aspects of the bearer services. The very first step is to agree on precise definitions of the basic terms (e.g., what is meant by a 'secure connection'?). Obviously, standard terms and description methods are needed.

However, there are increasing signs of community awareness of the related problems and a growing demand for their solution. By taking steps in improving risk analysis and modelling of security critical systems, CORAS will contribute a big step forward. Remember that security is also about increased privacy and unobstructed communication, in effect extending the general status of law and order to the information society. In this context, adequate security is a precondition for trust/acceptance of the computerised systems by the user communities. Therefore projects like CORAS will enable the realisation of long promised changes in our way of working and living. There will be many changes including teleworking, telemedicine and advanced electronic commerce. Preparing the infrastructure for electronic commerce is a particularly important EC policy, which will greatly benefit from improved risk analysis and modelling of security. In effect, a progress in the security area will improve the EU's ability to compete in the international marketplace and will have obvious benefits for its citizens.

Moreover, standardisation of security requirements may also contribute to extended trading between the countries, as a system manufactured in one country will satisfy security requirements in another country and can easily be sold there.

We find the IST framework well suited for promoting such enabling technologies and conduct co-ordinating development activities, as this cannot be initiated and driven from a single country.

b. Contribution to developing S&T co-operation at international level. European added value

c. Contribution to policy design or implementation

3.2.1 Contribution to Community social objectives

a. Improving the quality of life in the Community:

"***eEurope***", the political initiative to ensure the European Union fully benefits for generations to come from the imminent changes of the Information Society, has set three key objectives[1]:

- bringing every citizen, home and school, every business and administration into the digital age and online
- creating a digitally literate Europe, supported by an entrepreneurial culture ready to finance and develop new ideas
- ensuring the whole process is socially inclusive, builds consumer trust and strengthens social cohesion. Consumer confidence must be built if markets are to develop.

The development of the forthcoming Information Society involves the implementation, integration and utilisation of sophisticated and complex technological components. The resulting systems targeted to human users are getting harder for the community to grasp and yet a key objective is to have them widely used.

The gradual convergence of telecommunications and information systems permits a larger number of people to be involved in and make use of numerous technological possibilities. This in its turn drives people to gradually become more educated, demanding and insisting on vital matters such as "protection of privacy", "data integrity" and "secure transactions". As an example, cryptographic technology was for years an arcane topic restricted to a closed circle of people. It is only recently, with the growth of the Internet, that cryptography and on-line security has made it to the headlines.

There is a controversy that the advancement of Information Society must resolve. People are using more advanced, complicated and incomprehensible systems and yet they are expected to trust and have confidence to such systems that they do not fully understand. Security is the key to securing users trust and confidence, and thus to ensuring the further take-up of upcoming opportunities that the Information Society has to offer. The CORAS developed methodology will aid in solving the aforementioned problem. Its structured approach in modelling, specifying and risk-analysing security critical systems will improve the implementation and maintenance of secure systems and thus, strengthen the security assurance of large systems and reinforce the feeling of trust and confidence for their usage.

Legacy systems exist and novel ones are being developed in security critical domains such as defence, telecommunications, e-commerce and telemedicine. For such systems, a careful modelling, analytical specification and exhaustive analysis of potential risks and their consequences will ensure the accommodation and integration of all necessary security components. As a consequence such systems will be characterised as having their security validated and verified. Consumers by using these systems will gradually acknowledge the offered security and start trusting the system's support to dependability, confidentiality, integrity and privacy. This will lead to the creation of the desired secure-feeling that a modern Information Society is pursuing.

[1] Commission's initiative on *"eEurope: An Information Society for All"* for the extraordinary European Council of Lisbon on 23 – 24 March 2000.

Those systems that are commercially used will attract even more users. This will then spring the availability of more offers, something that will boost the market competition. Thus a chain is expected to be formed, where more and more people show trust in using security critical systems, thus increasing the demand, which leads in escalation of offers, which increases competition, resulting in excellence of service offers in terms of cost, quality and diversity. It can then be safely stated that this chain is for the benefit of the community.

Benefit to the community will be apparent and from the usage of those systems with non-commercial applications. These are heavily dependent on exchange, processing and assimilation of data information. It is imperative that information is securely exchanged within the nodes of such systems. By strengthening the security assurance of such systems, trust and confidence is built on the information exchanged, guaranteeing the data integrity, privacy and authenticity offered by the system. These characteristics will alleviate the reluctance of users for information disclosure. This will increase the throughput of information within such systems and will lead in offering more accurate and immediate results. The whole community is the winner out of such advancement.

To give an example, an advanced health-care system is examined. Such a system would gather, link together or generate statistical data from patient records. In a long time scale, the system will make it possible to visualise distributed patient information in a unified way and also gather, process and distribute activity data and epidemiological data from the entire health network in a given region. This is heavily dependent on patient record disclosure, data privacy, integrity and authenticity in order to produce valid results. This can be realised only if users become confident for the system's assurance in these important aspects.

There exist numerous examples of current as well as future systems that by offering security assurance will attract greater usage and will maximise the community benefit. However, the cornerstone for making this happen is to verify that all security considerations have been accommodated. This can only be done through a structured approach such as that promised by the CORAS project.

b. Provision of appropriate incentives for monitoring and creating jobs in the Community (including use and development of skills):

c. Supporting sustainable development, preserving and/or enhancing the environment (including use/conservation of resources):

3.3 Expected project impact

Overall Policy Impact[2]

EU Policy Goals	I SCALE OF EXPECTED IMPACT OVER THE NEXT 10 YEARS[3] -1 0 1 2 3	II Others Not applicable to project	II Project Impact too difficult to estimate
1. Improved sustainable economic development and growth, competitiveness	0		✔
2. Improved employment	0	✔	
3. Improved quality of life and health and safety	2		
4. Improved education	0	✔	
5. Improved preservation and enhancement of the environment	0	✔	

[2] Coordinator should respond to section I or, if appropriate, to section II. If the project has had no impact, a "0" should be entered in section I. Scores other than zero in section I will prompt a more detailed sub-question on a separate screen. However, you may access in any case the sub-questions by clicking on the symbol" Θ "following each main question.

[3] Indication for scale as follows: -1 represents negative impact, 0 no impact, 1 small positive impact, 2 medium positive impact, 3 is a strong positive impact

EU Policy Goals	I SCALE OF EXPECTED IMPACT OVER THE NEXT 10 YEARS[3] -1 0 1 2 3	II Others Not applicable to project	II Project Impact too difficult to estimate
6. Improved scientific and technological quality	0	✔	
7. Regulatory and legislative environment	0	✔	
8. Others _____	0		

Indicate your replies below by putting in each box the number corresponding to the score you chose:

1. Economic development and growth, competitiveness	**Scale of Expected Impacts over the next 10 years (2)**	
	By Project End -1 0 1 2 3	**After Project End** -1 0 1 2 3
a) Increased Turnover for project participants - national markets	0	1
- International markets	0	0
b) Increased Productivity for project participants	0	1
c) Reduced costs for project participants	0	1

2. Employment	**Scale of Expected Impacts over the next 10 years (2)**	
	By Project End -1 0 1 2 3	**After Project End** -1 0 1 2 3
a) Safeguarding of jobs	0	1
b) Net employment growth in projects participants staff	0	1
c) Net employment growth in customer and supply chains	0	1
d) Net employment growth in the European economy at large	0	0

3. Quality of Life and health and safety	Scale of Expected Impacts over the next 10 years (2)	
	By Project End -1 0 1 2 3	After Project End -1 0 1 2 3
a) Improved health care	0	1
b) Improved food, nutrition	0	0
c) Improved safety (incl. consumers and workers safety)	0	1
d) Improved quality of life for the elderly and disabled	0	0
e) Improved life expectancy	0	0
f) Improved working conditions	0	0
g) Improved child care	0	0
h) Improved mobility of persons	0	0

4. Improved education	Scale of Expected Impacts over the next 10 years (2)	
	By Project End -1 0 1 2 3	After Project End -1 0 1 2 3
a) Improved learning processes including lifelong learning	0	0
b) Development of new university curricula	0	2

5. Preservation and enhancement of the environment	**Scale of Expected Impacts over the next 10 years** (2)	
	By Project End -1 0 1 2 3	**After Project End** -1 0 1 2 3
a) Improved prevention of emissions	0	0
b) Improved treatment of emissions	0	0
c) Improved preservation of natural resources and cultural heritage	0	0
d) Reduced energy consumption	0	0

6. S&T quality	**Scale of Expected Impacts over the next 10 years** (2)	
	By Project End -1 0 1 2 3	**After Project End** -1 0 1 2 3
a) Production of new knowledge	2	1
b) Safeguarding or development of expertise in a research area	0	1
c) Acceleration of RTD, transfer or uptake	0	0
d) Enhance skills of RTD staff	0	1
e) Transfer expertise/know-how/technology	2	2
f) Improved access to knowledge-based networks	0	0
g) Identifying appropriate partners and expertise	0	1
h) Develop international S&T co-operation	0	1
i) Increased gender equality	0	0

7. Regulatory and legislative environment	Scale of Expected Impacts over the next 10 years (2)	
	By Project End -1 0 1 2 3	After Project End -1 0 1 2 3
a) Contribution to EU policy formulation	1	0
b) Contribution to EU policy implementation	0	1

8. Other (please specify)	Scale of Expected Impacts over the next 10 years (2)	
	By Project End -1 0 1 2 3	After Project End -1 0 1 2 3
a) Improved operational safety and security methodology for IT systems	1	2

I, the CORAS **project co-ordinator** confirm the published information contained in this part I of the TIP.

Signature: **Name: A. C. Price**

Date: 23/02/03 **Organisation: Telenor Communication II AS**

Part II - Description of results

Description of result 1

No. & TITLE OF THE RESULT

No.	Self-descriptive title of the result
1	***The CORAS Framework***

Contact person for this result:

Name	Dimitris Raptis
Position	
Organisation	INTRACOM
Address	19.5 Km Markopoulou Ave., GR-19002, Peiania, Athens, Greece
Telephone	+30 10 6677399
Fax	+30 10 6677312
E-mail	rap@intracom.gr
URL	http://www.intracom.gr
Specific Result URL	

SUMMARY

The main result of the CORAS project is the CORAS framework for model-based risk assessment of security-critical systems. This framework is characterised by:

- A methodology for model-based risk assessment integrating aspects from partly complementary risk assessment methods and state-of-the-art modelling methodology (see Result 2).
- A UML based specification language targeting security risk assessment (see Result 3).
- A library of reusable experience packages (see Result 4).
- A computerised platform providing two repositories; an assessment repository and a repository for the reusable experience packages (see Result 5).
- An XML mark-up for exchange of risk assessment data (see Result 6).
- A component for computerised vulnerability and threat management (see Result 7).

Please categorise the result using codes from Annex 1

Subject descriptors codes	598	321	129		

CURRENT STAGE OF DEVELOPMENT

Please tick one category only ✓

Scientific and/or Technical knowledge (Basic research)	☐
Guidelines, methodologies, technical drawings	✓
Software code	☐
Experimental development stage (laboratory prototype)	☐
Prototype/demonstrator available for testing	☐
Results of demonstration trials available	☐
Other (please specify.):	☐

DOCUMENTATION AND INFORMATION ON THE RESULT

List main information and documentation, stating whether public or confidential.

Documentation type	**Details (Title, ref. number, general description, language)**	**Status: *PU*=Public *CO*=Confidential**
Report	D2.4 Technical report providing templates and/or guidelines on how to adapt and extend existing risk analysis methodology for security critical systems	CO
Report	D3.7 Revisions of D3.2-6 after theoretical analysis and practical experience in integration and application trials	CO
Report	D4.4 Revised CORAS toolset, guidelines and full documentation	CO
Report	D4.5 Revision of D4.1 and D4.3 based on further experiences	CO
Report	D5.15 Trial results and assessment	PU

INTELLECTUAL PROPERTY RIGHTS

Type of IPR	**KNOWLEDGE:** **Tick a box and give the corresponding details (reference numbers, etc) if appropriate**					**Pre-existing know-how** **Tick a box and give the corresponding details (reference numbers, etc) if appropriate**	
	Current				**Foreseen**	**Tick**	**Details**
	Tick	**NoP [1)]**	**NoI [2)]**	**Details**	**Tick**		
Patent applied for	☐				☐	☐	
Patent granted	☐				☐	☐	
Patent search carried out	☐				☐	☐	
Registered design	☐				☐	☐	
Trademark applications	☐				☐	☐	
Copyrights	☐				☐	☐	
Secret know-how	☐				☐	☐	
Other - please specify:	☐				☐	☐	

1) Number of **P**riority (national) applications/patents

2) Number of **I**nternationally extended applications/patents

MARKET APPLICATION SECTORS

Please describe the possible sectors for application using the NACE classification in Annex 2.

Market application sectors	64	72	73l		

2.2. Quantified data about the result

Items (about the results)	**Actual current quantity [a]**	**Estimated (or future) quantity [b]**
Time to application / market (in months from the end of the research project)		6
Number of (public or private) entities potentially involved in the implementation of the result:	11	11
of which : number of SMEs :	1	1
of which : number of entities in third countries (outside EU) :	5	5
Targeted user audience: # of reachable people		>100 000
# of S&T publications (referenced publications only)	20	30
# of publications addressing general public (e.g. CD-ROMs, WEB sites)	10	15
# of publications addressing decision takers / public authorities / etc.	0	2
Visibility for the general public	No	

[a] *Actual current quantity = the number of items already achieved to date.*

[b] *Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve within the next 3 years.*

2.3. Further collaboration, dissemination and use of the result

COLLABORATIONS SOUGHT

Please tick appropriate boxes (✓) corresponding to your needs.

R&D	Further research or development	✓	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	☐
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing	✓	**INFO**	Information exchange	☐
JV	Joint venture	☐	**CONS**	Available for consultancy	☐
			Other	Standardisation	☐

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

The CORAS platform will be made available as open source. A major business-case is technical support and provision of content in the form of libraries of reusable experience packages.

PROFILE OF ADDITIONAL PARTNERS FOR FURTHER DISSEMINATION AND USE

Please, clearly describe the profile and the expected input from the external partner(s).

A vendor for a risk assessment tool or a UML CASE-tool, who would like to support the CORAS platform or parts of it, would be an ideal partner for further dissemination and use.

I confirm the information contained in part 2 of this Technological Implementation Plan and I authorise its dissemination to assist this search for collaboration.

Signature: **Name:** Dimitris Raptis

Date: **Organisation: INTRACOM**

Description of result 2

No. & TITLE OF RESULT

No.	Self-descriptive title of the result
2	***CORAS Methodology for Model-based Risk Assessment (MBRA)***

Contact person for this result:

Name	Bjørn Axel Gran
Position	Ph.D., Principal Research Scientist
Organisation	Institute for Energy Technology
Address	P.O. Box 173, N-1751 Halden, Norway
Telephone	+47 69212200
Fax	+47 69212440
E-mail	bjorn.axel.gran@hrp.no
URL	www.ife.no
Specific Result URL	

SUMMARY

Model based risk assessment (MBRA) builds on the concept of applying systems modelling when specifying and describing the systems to be assessed as an integrated part of the risk assessment.

The CORAS methodology for mode-based risk assessment is a risk assessment/management process based on the standardised modelling technique UML, the standards AS/NZS 4360:1999 "Risk Management" and ISO/IEC 17799-1: "Code of Practice for Information Security Management", and the Reference Model for Open Distributed Processing (RM-ODP). In particular, the CORAS MBRA incorporates adaptations and refinements of suitable, broadly used, generic risk analysis methodologies, and gives recommendations on how to apply the methodologies on systems models expressed in UML. The CORAS MBRA is also specialised towards assessment of security critical systems.

The CORAS methodology for mode-based risk assessment has been tested and turned out successfully at telemedicine and e-commerce systems through several trials. The benefit from the CORAS MBRA is that the assessment becomes effective due to a high degree of standardisation in describing the target of assessment and the increased level of reusability. At the same time the results become much easier to communicate to the different stakeholders.

Please categorise the result using codes from Annex 1

Subject descriptors codes	598	321	129		

CURRENT STAGE OF DEVELOPMENT

Please tick one category only ✓

Scientific and/or Technical knowledge (Basic research)	☐
Guidelines, methodologies, technical drawings	✓
Software code	☐
Experimental development stage (laboratory prototype)	☐
Prototype/demonstrator available for testing	☐
Results of demonstration trials available	☐
Other (please specify):	☐

DOCUMENTATION AND INFORMATION ON THE RESULT

List main information and documentation, stating whether public or confidential.

Documentation type	**Details (Title, ref. number, general description, language)**	**Status: *PU*=Public *CO*=Confidential**
Report	D2.4 Technical report providing templates and/or guidelines on how to adapt and extend existing risk analysis methodology for security critical systems	CO
Report	D4.4 Revised CORAS toolset guidelines and full documentation	CO
Paper	Yannis C. Stamatiou, Eva Henriksen, Mass Soldal Lund, Eva Mantzouranis, Michalis Psarros, Eva Skipenes, Nikos Stathiakos, Ketil Stølen. Experiences from using model-based risk assessment to evaluate the security of a telemedicine application. In the Proc. of Telemedicine in Care Delivery, 2002.	PU
Abstract	Eva Henriksen, Eva Skipenes. Experiences from applying the CORAS model-based risk assessment process in the telemedicine domain. In European Journal of Medical Research, vol. 7/ supplement I, page 33, Medical Scientific Publications, 2002.	PU
Abstract	Eva Skipenes, Eva Henriksen, Eva Mantzouranis. The CORAS approach for model-based risk analysis applied to the telemedicine domain. In Programme & Book of Abstracts 4th Nordic Congress on Telemedicine/Norsk Telemed, page 103, 2002.	PU
Paper	Ivan Djordevic, Cingwoei Gan, Eric Scharf, Raul Mondragon, Bjørn Axel Gran, Monica Kristiansen, Theo Dimitrakos, Ketil Stølen, Tom Arthur Opperud. Model-based risk management of security critical systems. In Proc. of Risk Analysis III, series: Management Information Systems, vol 5, WIT Press, 2002.	PU

Paper	Rune Fredriksen, Monica Kristiansen, Bjørn Axel Gran, Ketil Stølen, Tom Arthur Opperud, Theo Dimitrakos. The CORAS framework for a model-based risk management process. In Proc. Computer Safety, Reliability and Security (Safecomp 2002), LNCS 2434, pages 94-105, Springer, 2002.	PU
Paper	Jan Øyvind Aagedal, Folker den Braber, Theo Dimitrakos, Bjørn Axel Gran, Dimitris Raptis, Ketil Stølen. Model-based risk assessment to improve enterprise security. In Proc. Enterprise Distributed Object Communication (EDOC'2002), pages 51-62, IEEE Computer Society, 2002.	PU
Paper	PFolker den Braber, Theo Dimitrakos, Bjørn Axel Gran, Ketil Stølen, Jan Øyvind Aagedal. Model-based risk management using UML and UP. In Proc. Information Resources Management Association International Conference (IRMA'2002), pages 925-927, 2002.	PU
Paper	Siv-Hilde Houmb, Folker den Braber, Mass Soldal Lund, Ketil Stølen. Towards a UML profile for model-based risk assessment. In Proc. UML'2002 Satellite Workshop on Critical Systems Development with UML, pages 79-91, Munich University of Technology, 2002.	PU
Paper	Rune Fredriksen, Bjørn Axel Gran, Ketil Stølen, Ivan Djordjevic. Experiences from application of model-based risk assessment. To appear in Proc. European Conference on Safety and Reliability (ESREL'2003), 2003.	PU
Book Chapter	Ketil Stølen, Folker den Braber, Theo Dimitrakos, Rune Fredriksen, Bjørn Axel Gran, Siv-Hilde Houmb, Yannis C. Stamatiou, Jan Øyvind Aagedal. Model-based risk assessment in a component-based software engineering process: the CORAS approach to identify security risks. Chapter in book titled Business Component-Based Software Engineering edited by Franck Barbier, pages 189-207, Kluwer, 2003.	PU
Book Chapter	Folker den Braber, Theo Dimitrakos, Bjørn Axel Gran, Mass Soldal Lund, Ketil Stølen, Jan Øyvind Aagedal. The CORAS methodology: model-based risk management using UML and UP. Chapter in book titled UML and the Unified Process. IRM Press, 2003.	PU

INTELLECTUAL PROPERTY RIGHTS

Type of IPR	**KNOWLEDGE:** **Tick a box and give the corresponding details (reference numbers, etc) if appropriate**					**Pre-existing know-how** **Tick a box and give the corresponding details (reference numbers, etc) if appropriate**	
	Current				**Foreseen**	**Tick**	**Details**
	Tick	**NoP [1)]**	**NoI [2)]**	**Details**	**Tick**		
Patent applied for	☐				☐	☐	
Patent granted	☐				☐	☐	
Patent search carried out	☐				☐	☐	
Registered design	☐				☐	☐	
Trademark applications	☐				☐	☐	
Copyrights	☐				☐	☐	
Secret know-how	☐				☐	☐	
Other - please specify :	☐				☐	☐	

1) Number of **P**riority (national) applications/patents

2) Number of **I**nternationally extended applications/patents

MARKET APPLICATION SECTORS

Please describe the possible sectors for application using the NACE classification in Annex 2.

Market application sectors	64	72	85		

2.2. Quantified data about the result

Items (about the results)	**Actual current quantity [a]**	**Estimated (or future) quantity [b]**
Time to application / market (in months from the end of the research project)		1
Number of (public or private) entities potentially involved in the implementation of the result:	11	11
of which : number of SMEs:	5	5
of which : number of entities in third countries (outside EU) :	6	6
Targeted user audience: # of reachable people		> 100 000
# of S&T publications (referenced publications only)	2	?
# of publications addressing general public (e.g. CD-ROMs, WEB sites)	1	2
# of publications addressing decision takers / public authorities / etc.	9	> 10
Visibility for the general public	Yes	Yes

[a] *Actual current quantity = the number of items already achieved to date.*

[b] *Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve within the next 3 years.*

2.3. Further collaboration, dissemination and use of the result

The CORAS methodology for model-based risk assessment is together with the results from the IST-project DRIVE (IST-1999-12040) input to sub-proposals for" medical devices" for FP-6 (IP).

COLLABORATIONS SOUGHT

Please tick appropriate boxes (✓) corresponding to your needs.

R&D	Further research or	✓	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off	☐
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing	☐	**INFO**	Information exchange	✓
JV	Joint venture	☐	**CONS**	Available for consultancy	✓
			Other	(please specify)	☐

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

Please, clearly describe your input, the value and interest of the applications and the dissemination and use opportunities that you can offer to your potential partner.

The CORAS methodology for Model-Based Risk Assessment offers recommendations, as well as templates and guidelines, on how to perform risk assessment of security critical systems described by UML models. These recommendations can be further extended, refined or complemented, e.g. by investigating different model-based risk assessment approaches. The CORAS MBRA could also be refined to address not only security critical systems, but also safety related systems, or business critical systems. Further more, the experiences with the use of CORAS MBRA in dealing with critical systems can be of value for risk analysts, developers and decision makers. Finally, the CORAS methodology for model-based risk assessment can be applied as input for the revision of standards on risk management, security assessment and safety assessment.

PROFILE OF ADDITIONAL PARTNERS FOR FURTHER DISSEMINATION AND USE

Please, clearly describe the profile and the expected input from the external partner(s).

Users, such as risk analysts, developers or decision makers, who would like to apply the CORAS methodology for model-based risk assessment in their business.

Vendor of Risk Assessment tools who would like to give support for the CORAS methodology for model-based risk assessment in their tools.

I confirm the information contained in part 2 of this Technological Implementation Plan and I authorise its dissemination to assist this search for collaboration.

Signature: **Name: Bjørn Axel Gran**

Date: 23/02/03 **Organisation:** Institute for Energy Technology

Description of result 3

No. & TITLE OF RESULT

No.	Self-descriptive title of the result
3	***UML profile for Security Assessment***

Contact person for this result:

Name	Ketil Stølen
Position	Senior Scientist
Organisation	SINTEF
Address	P.O.Box 124 Blindern, N-0314 Oslo, Norway
Telephone	+47 22067897
Fax	+47 22067350
E-mail	ketil.stoelen@sintef.no
URL	www.sintef.no
Specific Result URL	

SUMMARY

The CORAS project has defined a UML profile for security risk assessment. UML is the most widely used specification language in the software industry today. A UML profile is an extension of the basic UML language targeting a more specialised application area. Hence, the CORAS UML profile is a UML based specification language targeting security risk assessment.

The CORAS UML profile is intended to support security risk assessment by:

- Allowing the target of evaluation (including the technical parts, the human users and relevant aspects of the surrounding enterprise) to be described at the right level of abstraction in a uniform manner, and thereby improve the quality of assessment results.
- Facilitating understanding and communication between the different groups of stakeholders to avoid misunderstandings and make the assessment process more effective.
- Document results and the assumptions on which these results depend to support reuse and reduce costs required for maintenance.

The CORAS UML profile defines a number of specialised UML diagrams and UML stereotypes that formalise the main CORAS concepts (such as "asset" and "threat").

Under the leadership of SINTEF a preliminary version of the CORAS UML profile has been submitted to the OMG in response to the Request for Proposals (RFP) titled “UML Profile for Modelling Quality of Service and Fault Tolerance Characteristics and Mechanisms" (submitted on September 9, 2002).

Please categorise the result using codes from Annex 1

Subject descriptors	598	400	129		

CURRENT STAGE OF DEVELOPMENT

Please tick one category only ✓

Scientific and/or Technical knowledge (Basic research)	☐
Guidelines, methodologies, technical drawings	✓
Software code	☐
Experimental development stage (laboratory prototype)	☐
Prototype/demonstrator available for testing	☐
Results of demonstration trials available	☐
Other (please specify.):	☐

DOCUMENTATION AND INFORMATION ON THE RESULT

List main information and documentation, stating whether public or confidential.

Documentation type	**Details(Title, ref. number, general description, language)**	**Status: *PU*=Public *CO*=Confidential**
Report	D3.7 Revisions of D3.2-6 after theoretical analysis and practical experience in integration and application trials	CO

INTELLECTUAL PROPERTY RIGHTS

Type of IPR	**KNOWLEDGE:** **Tick a box and give the corresponding details (reference numbers, etc) if appropriate**					**Pre-existing know-how** **Tick a box and give the corresponding details (reference numbers, etc) if appropriate**	
	Current				**Foreseen**	**Tick**	**Details**
	Tick	**NoP [1)]**	**NoI [2)]**	**Details**	**Tick**		
Patent applied for	☐				☐	☐	
Patent granted	☐				☐	☐	
Patent search carried out	☐				☐	☐	
Registered design	☐				☐	☐	
Trademark applications	☐				☐	☐	
Copyrights	☐				☐	☐	
Secret know-how	☐				☐	☐	
Other - please specify:	☐				☐	☐	

1) Number of **P**riority (national) applications/patents

2) Number of **I**nternationally extended applications/patents

MARKET APPLICATION SECTORS

Please describe the possible sectors for application using the NACE classification in Annex 2.

Market application sectors	64	72	73l		

2.2. Quantified data about the result

Items (about the results)	**Actual current quantity [a]**	**Estimated (or future) quantity [b]**
Time to application / market (in months from the end of the research project)		1
Number of (public or private) entities potentially involved in the implementation of the result:	2	?
of which : number of SMEs :	0	?
of which : number of entities in third countries (outside EU) :	2	?
Targeted user audience: # of reachable people	0	> 100 000
# of S&T publications (referenced publications only)	1	3
# of publications addressing general public (e.g. CD-ROMs, WEB sites)	0	2
# of publications addressing decision takers / public authorities / etc.	0	?
Visibility for the general public	No	No

[a] *Actual current quantity = the number of items already achieved to date.*

[b] *Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve within the next 3 years.*

2.3. Further collaboration, dissemination and use of the result

(Optional; to be completed if partner is willing to set up new collaborations, and seeking dissemination support from the CORDIS services.)

COLLABORATIONS SOUGHT

Please tick appropriate boxes (✓) corresponding to your needs.

R&D	Further research or development	✓	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	✓
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing	☐	**INFO**	Information exchange	☐
JV	Joint venture	☐	**CONS**	Available for consultancy	☐
			Other	Standardisation	✓

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

We will define the profile in accordance with the rules formalised by the UML 1.4 standard. The profile has no major value as such, but a tool supporting the profile may have major value. In order to make tools based on the profile attractive it is important that the profile gets acceptance among the UML community. A preliminary version of the profile has therefore been submitted in response to a call for proposals issued by the Object Management Group (OMG) - the organization responsible for the standardisation of the UML.

PROFILE OF ADDITIONAL PARTNERS FOR FURTHER DISSEMINATION AND USE

Please, clearly describe the profile and the expected input from the external partner(s).

A vendor for a risk assessment tool or a UML case-tool, who would like to support the profile, would be an ideal partner for further dissemination and use.

I confirm the information contained in part II of this Technological Implementation Plan and I authorise its dissemination to assist this search for collaboration.

Signature: **Name: Ketil Stølen**

Date: 23/02/03 **Organisation: SINTEF**

Description of result 4

No. & TITLE OF RESULT

No.	Self-descriptive title of the result
4	***Repository of Reusable Elements***

Contact person for this result:

Name	Siv Hilde Houmb
Position	Research Scientist
Organisation	Telenor Communication II AS
Address	Snarøyveien 31, 1330 Fornebu
Telephone	+47 913 07 714
Fax	+47 95 58 06 13
E-mail	siv-hilde.houmb@telenor.com
URL	
Specific Result URL	

SUMMARY

The repository of reusable elements is one of the major parts of the CORAS platform. The main purpose of the Reusable Elements Repository is to store reusable models, patterns and formats from already completed risk assessments. The reusable repository consist of two parts, one which is public and maintained by the CORAS partners, and one part which would typically be company internal maintained by the company in question. The public part of the repository will consist of general information related to risk assessment and security critical systems, in particular suitable for the Telemedicine and e-Commerce domain. This part of the repository will consist of models used to describe system components and results from risk assessments. The company internal part will consist of company confidential reusable elements from risk assessments, such as SWOT results, and models containing information reusable in later risk assessments, both on that particular system and on competitive systems. The approach is based on component-based software development paradigm and contributes to a more precise and cost effective risk assessment. All reusable elements will be stored and maintained as graphical representation using XML in the repository for reusable elements.

Please categorise the result using codes from Annex 1

Subject descriptors codes	598	320	129		

CURRENT STAGE OF DEVELOPMENT

Please tick one category only ✓

Scientific and/or Technical knowledge (Basic research)	☐
Guidelines, methodologies, technical drawings	☐
Software code	☐
Experimental development stage (laboratory prototype)	☐
Prototype/demonstrator available for testing	✓
Results of demonstration trials available	☐
Other (please specify.):	☐

DOCUMENTATION AND INFORMATION ON THE RESULT

List main information and documentation, stating whether public or confidential.

Documentation type	**Details(Title, ref. number, general description, language)**	**Status: *PU*=Public *CO*=Confidential**
Report	D4.3, Formats on integration	CO
Report	D3.3, Structure for storing and maintaining standard modelling components.	CO
Report	D3.5, Maintenance and consistency of risk assessments.	CO
Report	D3.6, Preliminary set of reusable experience packages	CO
Paper	Chingwoei Gan, Eric Scharf. Building an experience factory for a model-based risk analysis framework. To appear in Proc. 2nd German Workshop on Experience Management (GWEM'2003).	PU

INTELLECTUAL PROPERTY RIGHTS

Type of IPR	**KNOWLEDGE:** **Tick a box and give the corresponding details (reference numbers, etc) if appropriate**					**Pre-existing know-how** **Tick a box and give the corresponding details(reference numbers, etc) if appropriate**	
	Current				**Foreseen**	**Tick**	**Details**
	Tick	**NoP [1)]**	**NoI [2)]**	**Details**	**Tick**		
Patent applied for	☐				☐	☐	
Patent granted	☐				☐	☐	
Patent search carried out	☐				☐	☐	
Registered design	☐				☐	☐	
Trademark applications	☐				☐	☐	
Copyrights	☐				☐	☐	
Secret know-how	☐				☐	☐	
Other - please specify :	☐				☐	☐	

1) Number of **P**riority (national) applications/patents

2) Number of **I**nternationally extended applications/patents

MARKET APPLICATION SECTORS

Please describe the possible sectors for application using the NACE classification in Annex 2.

Market application sectors	64	72	85		

2.2. Quantified data about the result

Items (about the results)	**Actual current quantity [a]**	**Estimated (or future) quantity [b]**
Time to application / market (in months from the end of the research project)		1
Number of (public or private) entities potentially involved in the implementation of the result:	2	?
of which : number of SMEs :	1	?
of which : number of entities in third countries (outside EU) :	1	5
Targeted user audience: # of reachable people	0	
# of S&T publications (referenced publications only)	1	2
# of publications addressing general public (e.g. CD-ROMs, WEB sites)	1	5
# of publications addressing decision takers / public authorities / etc.		2
Visibility for the general public	No	Yes

[a] *Actual current quantity = the number of items already achieved to date.*

[b] *Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve within the next 3 years.*

2.3. Further collaboration, dissemination and use of the result

(Optional; to be completed if partner is willing to set up new collaborations, and seeking dissemination support from the CORDIS services.)

COLLABORATIONS SOUGHT

Please tick appropriate boxes (✓) corresponding to your needs.

R&D	Further research or development	☐	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	☐
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing	☐	**INFO**	Information exchange	✓
JV	Joint venture	☐	**CONS**	Available for consultancy	✓
			Other	(please specify)	☐

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

Please, clearly describe your input, the value and interest of the applications and the dissemination and use opportunities that you can offer to your potential partner.

We will generalise the models provided for the six trials in the two trial-domains within the CORAS project in order to provide reusable elements of both modules and issues related to security critical systems in general, and e-commerce and telemedicine in particular. The content in the repository will be extended in order to benefit the future users of the CORAS platform, who will benefit from the content in the repository, but also contribute and extend the content themselves in order to obtain a more resource effective risk analysis.

PROFILE OF ADDITIONAL PARTNER(S) FOR FURTHER DISSEMINATION AND USE

Please, clearly describe the profile and the expected input from the external partner(s).

A vendor or a consultant company, who would like to work with extending the content of the repository and work with generalising results from public available results related to risk assessment, would be an ideal partner for further dissemination and use. Even though the CORAS Platform will not be licensed there are possibilities to extend the functionality and content in the platform and for possible commercial dissemination around the platform, providing consultant service and providing helpdesk and maintenance service.

I confirm the information contained in part 2 of this Technological Implementation Plan and I authorise its dissemination to assist this search for collaboration.

Signature: **Name: Siv Hilde Houmb**

Date: 23/02/03 **Organisation: Telenor Communication II AS**

Description of result 5

No. & TITLE OF RESULT

No.	Self-descriptive title of the result
5	***CORAS Platform***

Contact person for this result:

Name	Michael Loupis
Position	Project Manager
Organisation	SOLINET GmbH Telecommunications
Address	Mittlerer Pfad 26, 70499, Stuttgart, Germany
Telephone	+ 49 711 1398 13 0
Fax	+ 49 711 866 12 40
E-mail	M.Loupis@SOLINET.com
URL	www.solinet.com
Specific Result URL	

SUMMARY

The CORAS platform for tool integration is the computerised part of the CORAS framework. Its core activity lies in the integration activity that aims to provide the underlying infrastructure for computerized integration of technical results as well as for external dissemination and exploitation.

The CORAS platform consists of two repositories: (1) The Assessment Repository storing the concrete results from already completed assessments and assessments in progress. (2) The Reusable Elements Repository storing reusable models, patterns and formats from already completed risk assessments.

In the development of the CORAS platform the emphasis is on XML (eXtensible Markup Language) based data-representations of existing XML formats as well as CORAS specific XML mark-up defined to meet the particular needs of the CORAS risk management process. The development of the CORAS platform also aims at creating the necessary interface(s) to the CORAS repository, which will allow users to "plug into" the platform in order to store/retrieve information they deem relevant.

The main benefits from the use of the CORAS platform are the following:

- Low investment cost: The rational of the CORAS platform is that there is not a specific "tool chain" needed in order to achieve the desired results. On the contrary, the user can choose among many commercial and non-commercial tools and integrate them in the CORAS platform. The fact that the data representation is based on XML reduces considerably the time and effort required for such a development.

- Time and effort reduction: The tool support provided by the CORAS platform considerably reduces the time required for the completion of a risk assessment by facilitating the reusability of models, patterns and formats from already completed risk assessments.

Please categorise the result using codes from Annex 1

Subject descriptors codes	152	220	320	321	

CURRENT STAGE OF DEVELOPMENT

Please tick one category only ✓

Scientific and/or Technical knowledge (Basic research)	☐
Guidelines, methodologies, technical drawings	☐
Software code	☐
Experimental development stage (laboratory prototype)	✓
Prototype/demonstrator available for testing	✓
Results of demonstration trials available	☐
Other (please specify.):	☐

DOCUMENTATION AND INFORMATION ON THE RESULT

List main information and documentation, stating whether public or confidential.

Documentation type	**Details(Title, ref. number, general description, language)**	**Status:** ***PU*****=Public** ***CO*****=Confidential**
CORAS deliverable	D4.3: Formats of integration	CO

INTELLECTUAL PROPERTY RIGHTS

Type of IPR	**KNOWLEDGE:** **Tick a box and give the corresponding details (reference numbers, etc) if appropriate**					**Pre-existing know-how** **Tick a box and give the corresponding details (reference numbers, etc) if appropriate**	
	Current				**Foreseen**	**Tick**	**Details**
	Tick	**NoP [1)]**	**NoI [2)]**	**Details**	**Tick**		
Patent applied for	☐				☐	☐	
Patent granted	☐				☐	☐	
Patent search carried out	☐				☐	☐	
Registered design	☐				☐	☐	
Trademark applications	☐				☐	☐	
Copyrights	☐				☐	☐	
Secret know-how	☐				☐	☐	
Other - please specify:	☐				☐	☐	

1) Number of **P**riority (national) applications/patents

2) Number of **I**nternationally extended applications/patents

MARKET APPLICATION SECTORS

Please describe the possible sectors for application using the NACE classification in Annex 2.

Market application sectors	72	74			

2.2. Quantified data about the result

Items (about the results)	**Actual current quantity [a]**	**Estimated (or future) quantity [b]**
Time to application / market (in months from the end of the research project)		24
Number of (public or private) entities potentially involved in the implementation of the result:		
of which : number of SMEs :		
of which : number of entities in third countries (outside EU) :		0
Targeted user audience: # of reachable people		
# of S&T publications (referenced publications only)		10
# of publications addressing general public (e.g. CD-ROMs, WEB sites)		3
# of publications addressing decision takers / public authorities / etc.		10
Visibility for the general public	Yes	

[a] *Actual current quantity = the number of items already achieved to date.*

[b] *Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve within the next 3 years.*

2.3. Further collaboration, dissemination and use of the result

(Optional; to be completed if partner is willing to set up new collaborations, and seeking dissemination support from the CORDIS services.)

COLLABORATIONS SOUGHT

Please tick appropriate boxes (✓) corresponding to your needs.

R&D	Further research or development	✓	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	☐
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing	✓	**INFO**	Information exchange	☐
JV	Joint venture	☐	**CONS**	Available for consultancy	☐
			Other	(please specify)	☐

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

Please, clearly describe your input, the value and interest of the applications and the dissemination and use opportunities that you can offer to your potential partner.

The CORAS platform is designed and implemented in a way that permits the inclusion of tools developed by different vendors. Potential partners would be interested in integrating their tools in the CORAS platform.

PROFILE OF ADDITIONAL PARTNERS FOR FURTHER DISSEMINATION AND USE

Please, clearly describe the profile and the expected input from the external partner(s).

Potential partners are software houses developing tools for risk analysis, UML, vulnerability assessment and threat management that can be included in the CORAS platform.

I confirm the information contained in part 2 of this Technological Implementation Plan and I authorise its dissemination to assist this search for collaboration.

Signature: **Name:** Michael Loupis

Date: 23/02/03 **Organisation:** SOLINET

Description of result 6

No. & TITLE OF RESULT

No.	Self-descriptive title of the result
6	***XML format for representation of Risk Assessment***

Contact person for this result:

Name	Theodosis Dimitrakos
Position	
Organisation	CLRCL
Address	Oxfordshire, OX11 0QX, UK
Telephone	+44 12 35 44 57 10
Fax	+44 12 35 44 58 31
E-mail	T.Dimitrakos@rl.ac.uk
URL	http://www.bitd.clrc.ac.uk/
Specific Result URL	

SUMMARY

In the absence of any standardised meta-data format for representing information related to Risk Assessment, the CORAS consortium has decided to initiate the development of an XML format for representing Risk Assessment information. Such meta-data description of core Risk Assessment data are being used for the purpose of consistency checking between different items of the repositories provided by the CORAS tool inclusion platform.

At present, we are developing XML-based information models for the core elements of the different risk analysis methods used in CORAS. We intend to evaluate this experience of taking advantage of such meta-data description with the view of extending the CORAS approach in order to achieve in-depth data-oriented tool integration among Risk Assessment tools and Systems Modelling tools or tools for vulnerability and threat management.

Subject to a satisfactory outcome of research in this direction, we will coordinate the communication of the report to the World Wide Web Consortium (W3C) with a request to be considered for publication by W3C as a Note, following the W3C member submission process (summarised in the appendix). This is the typical route to follow, should the consortium wish to have ideas that are developed outside of W3C Activities published by W3C.

However, it has to be clarified that submission process is **not** a means by which Members ask for "ratification" of these documents as W3C Recommendations. There is no requirement or guarantee that the technology that is part of an acknowledged submission request will receive further consideration by W3C (e.g., by a W3C Working Group). Still, this submission process allows the W3C Team to review proposed technology and accurately relay the status of submission requests to the media, and provide a means of communicating results developed outside W3C to the W3C Team through some W3C member.

Please categorise the result using codes from Annex 1

Subject descriptors codes					

CURRENT STAGE OF DEVELOPMENT

Please tick one category only ✓

Scientific and/or Technical knowledge (Basic research)	✓
Guidelines, methodologies, technical drawings	✓
Software code	☐
Experimental development stage (laboratory prototype)	✓
Prototype/demonstrator available for testing	☐
Results of demonstration trials available	☐
Other (please specify.):	☐

DOCUMENTATION AND INFORMATION ON THE RESULT

List main information and documentation, stating whether public or confidential.

Documentation type	**Details(Title, ref. number, general description, language)**	**Status:** ***PU*****=Public** ***CO*****=Confidential**
CORAS deliverable	D4.3: Formats of integration	CO
CORAS deliverable	D4.4 Revised CORAS toolset, guidelines and full documentation	CO
CORAS deliverable	D4.5 Revision of D4.1 and 4.3 based on further experiences	CO

INTELLECTUAL PROPERTY RIGHTS

Type of IPR	**KNOWLEDGE:** **Tick a box and give the corresponding details (reference numbers, etc) if appropriate**					**Pre-existing know-how** **Tick a box and give the corresponding details(reference numbers, etc) if appropriate**	
	Current				**Foreseen**	**Tick**	**Details**
	Tick	**NoP [1)]**	**NoI [2)]**	**Details**	**Tick**		
Patent applied for	☐				☐	☐	
Patent granted	☐				☐	☐	
Patent search carried out	☐				☐	☐	
Registered design	☐				☐	☐	
Trademark applications	☐				☐	☐	
Copyrights	☐				☐	☐	
Secret know-how	☐				☐	☐	
Other - please specify:	☐				☐	☐	

1) Number of **P**riority (national) applications/patents

2) Number of **I**nternationally extended applications/patents

MARKET APPLICATION SECTORS

Please describe the possible sectors for application using the NACE classification in Annex 2.

Market application sectors					

2.2. Quantified data about the result

Items (about the results)	**Actual current quantity [a]**	**Estimated (or future) quantity [b]**
Time to application / market (in months from the end of the research project)		36
Number of (public or private) entities potentially involved in the implementation of the result:		n/a
of which : number of SMEs :		n/a
of which : number of entities in third countries (outside EU) :		n/a
Targeted user audience: # of reachable people		> 100 000
# of S&T publications (referenced publications only)		10
# of publications addressing general public (e.g. CD-ROMs, WEB sites)		5
# of publications addressing decision takers / public authorities / etc.		2
Visibility for the general public	Yes / No	

[a] *Actual current quantity = the number of items already achieved to date.*

[b] *Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve within the next 3 years.*

2.3. Further collaboration, dissemination and use of the result

The increasing complexity of today's IT dependent systems urges the improvement of existing methods for analysing systems and their models in order to increase the likelihood that all possible threats and vulnerabilities are taken into consideration. Such an improvement can be achieved by

1. Combining different complementary risk assessment methodologies with respect to the system architecture, implementation, and use;

2. Assessing all different aspects of dependability (e.g. availability, safety, security, survivability, etc.) and their impact on each other with respect to the system architecture implementation, and use;

3. Providing light-weight and extensible tool inclusion frameworks supporting the co-use and/or integration of risk analysis, system design and real-time monitoring tools.

The fact that qualitative methodologies for analysing risk lack the ability to account for the dependencies between events, but are effective in identifying potential hazards and failures in trust

within the system, whereas tree-based techniques take into consideration the dependencies between each event provides evidence supporting item (1) above.

The findings of various dependability roadmap projects support the view of item (2) above: The IT community have come to realise that all aspects of dependability should be considered together as a coherent whole. In particular, given the model of an information system a coherent analysis of all aspects of dependability is by far more effective than the sum of the analyses of each aspect in isolation.

As for item (3), the complexity of today's IT dependent systems increases the complexity of the risk analysis tasks and demands for the co-use and/or integration various tools providing clear and easy-to explore view of the system at hand, as well as, tools supporting specific risk analysis methods and tasks. In addition to a plethora of system design, modelling and system analysis tools, the significant number of specialised risk assessment tools indicates that it is more cost-efficient to integrate specialised tools (which have been developed and test over decades and people are familiar with) rather than re-invent tool support in the context of an integrated methodology. CORAS experience has shown however that a tightly integrated tool-chain is not necessary the best solution: Different enterprises have often their own legacy systems for design and/or risk assessment while the design and risk assessment tool specifications often change without preserving backwards compatibility. Instead, one can provide a "loose" tool inclusion platform based on standardised representations of modelling and risk assessment meta-data which allow users to plug-in their preferred tools using commonly agreed or standardised and extensible exchange formats.

The new Integrated Project instrument presents an opportunity to build a programme of the required scale, breath of vision and expertise in order to overcome the compromises to the effectiveness of risk assessment introduced at the boundaries of partial solutions addressing a single aspect of dependability, while it provides a useful context for developing a tool integration platform in close collaboration with method integration.

At present, we are developing XML-based information models for the core elements of the different risk analysis methods used in CORAS. We intend to evaluate this experience of taking advantage of such meta-data description with the view of extending the CORAS approach in order to achieve in-depth data-oriented tool integration among Risk Assessment tools and Systems Modelling tools or tools for vulnerability and threat management, as well as extending the approach so as to support jointly assessing different aspects of dependability.

Subject to a satisfactory outcome of research in this direction, we will coordinate the communication of the report to the World Wide Web Consortium (W3C) with a request to be considered for publication by W3C as a Note, following the W3C member submission process (summarised in the appendix). This is the typical route to follow, should the consortium wish to have ideas that are developed outside of W3C Activities published by W3C.

As CLRC-RAL hosts the UK W3C office which participates in monthly meetings across all offices, and the Head of Office being a W3C Team member, should leverage be required to progress a submission to a W3C working Group etc. then, through the UK W3C Office, we can exert that leverage.

COLLABORATIONS SOUGHT

Please tick appropriate boxes (✓) corresponding to your needs.

R&D	Further research or development	✓	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	☐
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	✓
MKT	Marketing	☐	**INFO**	Information exchange	☐
JV	Joint venture	☐	**CONS**	Available for consultancy	✓
			Other	(please specify) standardisation	✓

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

Please, clearly describe your input, the value and interest of the applications and the dissemination and use opportunities that you can offer to your potential partner.

CORAS experience has shown however that a tightly integrated tool-chain for Model-based Risk Assessment is not necessary the best solution: Different enterprises have often their own legacy systems for design and/or risk assessment while the design and risk assessment tool specifications often change without preserving backwards compatibility. Instead, one can provide a "loose" tool inclusion platform based on standardised representations of modelling and risk assessment meta-data which allow users to plug-in their preferred tools using commonly agreed or standardised and extensible exchange formats.

At present, we are developing XML-based information models for the core elements of the different risk analysis methods used in CORAS. We intend to evaluate this experience of taking advantage of such meta-data description with the view of extending the CORAS approach in order to achieve in-depth data-oriented tool integration among Risk Assessment tools and Systems Modelling tools or tools for vulnerability and threat management, as well as extending the approach so as to support jointly assessing different aspects of dependability.

Subject to a satisfactory outcome of research in this direction, we will coordinate the communication of the report to the World Wide Web Consortium (W3C) with a request to be considered for publication by W3C as a Note, following the W3C member submission process (summarised in the appendix). This is the typical route to follow, should the consortium wish to have ideas that are developed outside of W3C Activities published by W3C.

PROFILE OF ADDITIONAL PARTNERS FOR FURTHER DISSEMINATION AND USE

Please, clearly describe the profile and the expected input from the external partner(s).

Users who would like to participate in further experimentation and evaluation of tools supporting Model-based Risk Analysis.

Risk Analysts; Researchers in the Semantic Web area.

Vendor of Risk Assessment and Modelling CASE tools who would like to support open source expansions of tools included in their tool chains.

I confirm the information contained in part 2 of this Technological Implementation Plan and I authorise its dissemination to assist this search for collaboration.

Signature: **Name:** Theodosis Dimitrakos

Date: 23/02/03 **Organisation: RAL**

Description of result 7

No. & TITLE OF RESULT

No.	Self-descriptive title of the result
7	***Vulnerability and Threat Management Component***

Contact person for this result:

Name	Michael Loupis
Position	Project Manager
Organisation	SOLINET GmbH Telecommunications
Address	Mittlerer Pfad 26, 70499, Stuttgart, Germany
Telephone	+ 49 711 1398 13 0
Fax	+ 49 711 866 12 40
E-mail	M.Loupis@SOLINET.com
URL	www.solinet.com
Specific Result URL	

SUMMARY

The increasing security incidents that result from network attacks impose, among other security practices, the use of vulnerability assessment tools (i.e. scanners) and threat management (i.e. intrusion detection) tools. In CORAS methodology we propose the use of documentation and logs form the above categories of tools, in the following activities:

- Threat identification. Valuable information on potential threats can be gathered by the review of attack-alerts logged by intrusion detection tools. These logs provide a source of information on security incidents that posed a threat to the system security in the past.
- Vulnerability identification. The main results of vulnerability assessment tools are the identification of the known vulnerabilities associated to the current versions of the operating systems and services.
- Risk Treatment. The vulnerability assessment reports also practical guidance on how to make the system less vulnerable to potential threats.

The above proposals were successfully tested for the vulnerability assessment tools during a trial performed in the TeleCardiology service.

Please categorise the result using codes from Annex 1

Subject descriptors codes	424	342			

CURRENT STAGE OF DEVELOPMENT

Please tick one category only ✓

Scientific and/or Technical knowledge (Basic research)	☐
Guidelines, methodologies, technical drawings	✓
Software code	☐
Experimental development stage (laboratory prototype)	☐
Prototype/demonstrator available for testing	☐
Results of demonstration trials available	✓
Other (please specify.):	☐

DOCUMENTATION AND INFORMATION ON THE RESULT

List main information and documentation, stating whether public or confidential.

Documentation type	**Details(Title, ref. number, general description, language)**	**Status: *PU*=Public *CO*=Confidential**
CORAS Deliverable	D4.2: Evaluation of different tool-chains	CO
CORAS Deliverable	D2.3: Guidelines and Templates for Model-based Risk Assessment	CO
CORAS Deliverable	D5.7: First risk assessment report for TeleCardiology	CO
CORAS Deliverable	D5.8: Second Assessment of the CORAS methodology	CO

INTELLECTUAL PROPERTY RIGHTS

Type of IPR	**KNOWLEDGE:** **Tick a box and give the corresponding details (reference numbers, etc) if appropriate**					**Pre-existing know-how** **Tick a box and give the corresponding details (reference numbers, etc) if appropriate**	
	Current				**Foreseen**	**Tick**	**Details**
	Tick	**NoP [1)]**	**NoI [2)]**	**Details**	**Tick**		
Patent applied for	☐				☐	☐	
Patent granted	☐				☐	☐	
Patent search carried out	☐				☐	☐	
Registered design	☐				☐	☐	
Trademark applications	☐				☐	☐	
Copyrights	☐				☐	☐	
Secret know-how	☐				☐	☐	
Other - please specify:	☐				☐	☐	

1) Number of **P**riority (national) applications/patents

2) Number of **I**nternationally extended applications/patents

MARKET APPLICATION SECTORS

Please describe the possible sectors for application using the NACE classification in Annex 2.

Market application sectors	72	731			

2.2. Quantified data about the result

Items (about the results)	**Actual current quantity [a]**	**Estimated (or future) quantity [b]**
Time to application / market (in months from the end of the research project)		1
Number of (public or private) entities potentially involved in the implementation of the result:		
of which : number of SMEs :		1
of which : number of entities in third countries (outside EU) :		0
Targeted user audience: # of reachable people		
# of S&T publications (referenced publications only)		2
# of publications addressing general public (e.g. CD-ROMs, WEB sites)		1
# of publications addressing decision takers / public authorities / etc.		5
Visibility for the general public	Yes	

[a] *Actual current quantity = the number of items already achieved to date.*

[b] *Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve within the next 3 years.*

2.3. Further collaboration, dissemination and use of the result

(Optional; to be completed if partner is willing to set up new collaborations, and seeking dissemination support from the CORDIS services.)

COLLABORATIONS SOUGHT

Please tick appropriate boxes (✓) corresponding to your needs.

R&D	Further research or development	✓	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	☐
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing	✓	**INFO**	Information exchange	☐
JV	Joint venture	☐	**CONS**	Available for consultancy	✓
			Other	(Please specify)	☐

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

Please, clearly describe your input, the value and interest of the applications and the dissemination and use opportunities that you can offer to your potential partner.

The collection of sufficient data from vulnerability assessment and threat management tools used during past risk assessments can be used for the frequency (likelihood) estimation of potential attacks. Given the absence of reliable statistics relevant to computer security risks, the use of the CORAS repository as source of information will be valuable to the risk analysts. This information could also be shared among organisations that use the CORAS platform.

PROFILE OF ADDITIONAL PARTNERS FOR FURTHER DISSEMINATION AND USE

Please, clearly describe the profile and the expected input from the external partner(s).

Potential partners are organisations interested in collecting data relevant to computer security risks

I confirm the information contained in part 2 of this Technological Implementation Plan and I authorise its dissemination to assist this search for collaboration.

Signature: **Name:** Michael Loupis

Date: **Organisation:** SOLINET GmbH Telecommunications

Part III - Description of intentions (per partner)

The rest of the document contains Part III of TIP for those partners that decided to submit the document via the project coordinator. The TIP for the following partners are included, whereas, the rest of partners decided to keep Part III of the TIP document confidential and want to submit directly to the commission.

- INTRACOM
- IFE
- NR
- SINTEF
- NCT
- RAL
- QMW
- CTI

Notes:

a) Telenor and SOLINET consider their implementation plan confidential and decided to submit their intention directly to the EU Commission.

b) FORTH does cannot submit its implementation plan as its inclusion in the CORAS consortium has not yet been officially approved. FORTH will therefore include its TIP intentions when D7.4 is revised at the end of the project.

CONTRACT NUMBER:	**IST-2000-25031**
PARTNER's NAME:	**INTRACOM S.A.**

CONTACT PERSON:

Name	D. Raptis
Position/Title	System Analyst
Organisation	INTRACOM S.A.
Address	19.5 Km Markopoulou Ave., GR-19002, Peania, Athens, Greece.
Telephone	+30 210 6677399
Fax	+30 210 6677312
E-mail	drap@intracom.gr

Number, TITLE AND BRIEF DESCRIPTION OF MAIN RESULT(S)

1	The CORAS Framework
2	*CORAS methodology for Model-based Risk Assessment (MBRA)*
3	UML profile for Security Assessment
4	Repository of Reusable Elements
5	CORAS Platform
6	XML format for representation of Risk Assessment
7	Vulnerability and Threat Management Component

FOR EACH MAIN RESULT:

TIMETABLE OF THE USE AND DISSEMINATION ACTIVITIES WITHIN THE NEXT 3 YEARS AFTER THE END OF THE PROJECT

Mention the use and dissemination related activities, the main associated partners, the related milestones and give an indicative timescale		
Activity	**Brief description of the activity, including main milestones and deliverables (and how it relates to data in sections 2.2 and 3.2).**	**Timescale (months)**

Internal Usage	It is expected that the CORAS Framework for MBRA will be suitable for internal deployment in the Software Development processes in the company. As software in the Company is developed following Object-Oriented methodologies, it is expected that the CORAS Framework will be relative easy incorporated in the current practises. Separate deployment of each component of the CORAS framework however, depending on the specific needs, is also foreseen. For example the CORAS guidelines may be included in a Quality Manual without the need for the COARS Platform. Further, the dissemination of the CORAS framework will assist in raising awareness on considering security aspects of a system at the early stages of its development. (Results 1-7)	6-24
Extension/Specialisation of CORAS Framework with specific examples.	The CORAS Guidelines may be extended or specialised, incorporating examples extracted from the e-Commerce Trials or customised examples, to clarify or illustrate the specific aspects addressed by each part of the Framework. This will assist the Software Engineers, as users of the framework, to relate it with their experiences and incorporate it within their current practices.	3-12
Exploitation of assessment of e-Commerce platform functionalities	The security provided by the e-Commerce platform constitutes an important marketing feature for the platform. The dissemination of the platform can be strengthened by advertising the assessment of various incorporated security-critical mechanisms via the application of the CORAS framework.	6-24
Reuse of the assessed mechanisms of the platform	The functionalities assessed in the e-Commerce trials constitute relatively independent security-critical components of the platform. These functionalities may therefore become independent reusable components should the suitable opportunity arise to provide security critical components with similar functionalities.	6-36

FOREseen COLLABORATIONS WITH OTHER ENTITIES

Please tick appropriate boxes (✓) corresponding to your most probable follow-up.

R&D	Further research or development	☐	**FIN**	Financial support	☐
LIC	Licence agreement	✓	**VC**	Venture capital/spin-off funding	☐
MAN	Manufacturing agreement	✓	**PPP**	Private-public partnership	☐
MKT	Marketing agreement/Franchising	☐	**INFO**	Information exchange, training	✓
JV	Joint venture	☐	**CONS**	Available for consultancy	✓
			Other	(please specify)	☐

3.2: Quantified data for each partner's main result

Items	Currently achieved quantity [a]	Estimated future quantity [b]
Economic impacts (in EURO)	?	?
# of licenses issued (within EU)	0	0
# of licenses issued (outside EU)	0	0
Total value of licenses (in EURO)	0	0
# of entrepreneurial actions (start-up company, joint ventures…)	0	0
# of direct jobs created [c]	0	0
# of direct jobs safeguarded [c]	0	0
# of direct jobs lost	0	0

[a] *The added value or the number of items already achieved to date.*

[b] *Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve in the future (i.e. expectations within the next 3 years following the end of the project).*

[c] *"Direct jobs" means jobs within the partner involved. Research posts are to be excluded from the jobs calculation*

 # = number of ...

I confirm the information contained in part 3 of this Technological Implementation Plan and I certify that these are currently our main exploitation intentions

Signature: **Name: D. Raptis**

Date: Feb. 11, 2003

insert correct date !

CONTRACT NUMBER:	**IST-2000-25031**
PARTNER's NAME:	**Institute for Energy Technology (IFE)**

CONTACT PERSON:

Name	Bjørn Axel Gran
Position/Title	Principal Research Scientist/Ph.D.
Organisation	Institute for Energy Technology
Address	P.O.Box 173, NO-1751 Halden
Telephone	+47 69212200
Fax	+47 69212440
E-mail	bjorn.axel.gran@hrp.no

Number, TITLE AND BRIEF DESCRIPTION OF MAIN RESULTS

No.	Title	Description
1	CORAS Framework	Dissemination of the CORAS Framework for supporting the activities on main result 2.
2	*CORAS methodology for Model-based Risk Assessment (MBRA)*	Dissemination and use of the CORAS methodology for Model-Based Risk Assessment. Continue the investigation of the potential use of system modelling in general and the applied method in particular, as a basis for risk assessment. Additionally, investigate the applicability of the proposed method in covering safety aspects in safety and security critical systems.
3	*UML profile for Security Assessment*	-
4	*Repository of Reusable Elements*	Dissemination and use of the repository of reusable elements for supporting the activities on main results 2.
5	*CORAS Platform*	Dissemination, use and promotion of the CORAS Platform for supporting the activities on main results 2.
6	*XML format for representation of Risk Assessment*	-
7	*Vulnerability and Threat Management Component*	-

FOR MAIN RESULT 1:

TIMETABLE OF THE USE AND DISSEMINATION ACTIVITIES WITHIN THE NEXT 3 YEARS AFTER THE END OF THE PROJECT

Mention the use and dissemination related activities, the main associated partners, the related milestones and give an indicative timescale		
Activity	**Brief description of the activity, including main milestones and deliverables (and how it relates to data in sections 2.2 and 3.2).**	**Timescale (months)**
Dissemination of the CORAS framework.	Dissemination of the CORAS framework in order to support the activities for main result 2.	**(0-36)**

FORESEEN COLLABORATIONS WITH OTHER ENTITIES

Please tick appropriate boxes (✓) corresponding to your most probable follow-up.

R&D	Further research or development	✓	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	☐
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing agreement/Franchising	☐	**INFO**	Information exchange, training	✓
JV	Joint venture	☐	**CONS**	Available for consultancy	✓
			Other	(please specify)	☐

<u>FOR MAIN RESULT 2:</u>

TIMETABLE OF THE USE AND DISSEMINATION ACTIVITIES WITHIN THE NEXT 3 YEARS AFTER THE END OF THE PROJECT

Mention the use and dissemination related activities, the main associated partners, the related milestones and give an indicative timescale		
Activity	**Brief description of the activity, including main milestones and deliverables (and how it relates to data in sections 2.2 and 3.2).**	**Timescale (months)**
Dissemination and use of the CORAS methodology for model-based risk assessment in the OECD Halden Reactor Project	The OECD Halden Reactor Project (HRP) is an international research institution with participation from 18 countries in Europe, Asia and America. The project is hosted by IFE and runs on triennial contracts. A main research topic in the section for Safety and Reliability of Computerised Systems at IFE is risk assessment, with particular emphasis on critical software based systems. Model-based risk assessment is highlighted in the programme for the next three years (2003-2005). The plan is to continue the activity initiated in 2002 to investigate the potential use of system modelling as a basis for risk analysis of safety related systems. The application of CORAS methodology as one among model-based risk assessment approaches will be considered. Additionally, the prospects of using a model-based assessment method for covering safety aspects of especially nuclear power plants will be investigated. M1: EHPG meeting in 2004, Report, February 2004 M2: EHPG meeting in 2005, Report, May 2005	**(0-30)**

Tutorial on the CORAS methodology for model-based risk Assessment	In order to promote the use of the CORAS methodology for model-based risk assessment (CORAS MBRA), and ease the usability of CORAS MBRA there will be a need for tutorials and course-material on CORAS MBRA. Tutorials and course material will be made in co-operation with the Østfold University College and NTNU, Norway. M1: Tutorial on CORAS MBRA, Presentation, September 2003 M2: Course-material on CORAS MBRA, Report, August 2004 M3: Draft-book on CORAS MBRA, Draft of book, 2005	**(0-36)**
CORAS MBRA user group in Norway	Although the CORAS MBRA is one of the results of CORAS, it is expected that there will be a need for exchanging experiences on the use of CORAS MBRA. Together with Telenor and NCT, IFE will take responsibility for establishing a CORAS MBRA user group. M1: Establish a CORAS MBRA user group in Norway, meeting, 2003 M2: Annual meetings of the user group, 2004, 2005.	**(0-36)**
Consultancy work	IFE will make use of the experiences on model based risk assessment in future consultancy work. Sectors, where IFE is doing consultancy work are within nuclear, petroleum, and transport. Other sectors may also be exploited.	**(0-36)**

FORESEEN COLLABORATIONS WITH OTHER ENTITIES

Please tick appropriate boxes (✓) corresponding to your most probable follow-up.

R&D	Further research or development	✓	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	☐
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing agreement/Franchising	☐	**INFO**	Information exchange, training	✓
JV	Joint venture	☐	**CONS**	Available for consultancy	✓
			Other	(please specify)	☐

FOR MAIN RESULT 4:

TIMETABLE OF THE USE AND DISSEMINATION ACTIVITIES WITHIN THE NEXT 3 YEARS AFTER THE END OF THE PROJECT

Mention the use and dissemination related activities, the main associated partners, the related milestones and give an indicative timescale		
Activity	**Brief description of the activity, including main milestones and deliverables (and how it relates to data in sections 2.2 and 3.2).**	**Timescale (months)**
Dissemination and use of the repository of reusable elements.	Dissemination and use of the repository of reusable elements in order to support the activities for main result 2.	**(0-36)**

FORESEEN COLLABORATIONS WITH OTHER ENTITIES

Please tick appropriate boxes (✓) corresponding to your most probable follow-up.

R&D	Further research or development	✓	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	☐

MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing agreement/Franchising	☐	**INFO**	Information exchange, training	✓
JV	Joint venture	☐	**CONS**	Available for consultancy	☐
			Other	(please specify)	☐

FOR MAIN RESULT 5:

TIMETABLE OF THE USE AND DISSEMINATION ACTIVITIES WITHIN THE NEXT 3 YEARS AFTER THE END OF THE PROJECT

Mention the use and dissemination related activities, the main associated partners, the related milestones and give an indicative timescale		
Activity	**Brief description of the activity, including main milestones and deliverables (and how it relates to data in sections 2.2 and 3.2).**	**Timescale (months)**
Dissemination and use of the CORAS platform.	Dissemination and use of the CORAS platform in order to support the activities for main result 2.	**(0-36)**
Promotion of the CORAS Platform within the OECD Halden Reactor Project	Promote the CORAS platform in relation to the research activity related to main result 2.	**(0-36)**

FORESEEN COLLABORATIONS WITH OTHER ENTITIES

Please tick appropriate boxes (✓) corresponding to your most probable follow-up.

R&D	Further research or development	✓	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	☐
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing agreement/Franchising	☐	**INFO**	Information exchange, training	✓
JV	Joint venture	☐	**CONS**	Available for consultancy	☐
			Other	(please specify)	☐

3.2: Quantified data for each partner's main result

Items	**Currently achieved quantity** [a]	**Estimated future quantity** [b]
Economic impacts (in EURO)	?	?
# of licenses issued (within EU)	0	0
# of licenses issued (outside EU)	0	0
Total value of licenses (in EURO)	0	0
# of entrepreneurial actions (start-up company, joint ventures…)	0	0
# of direct jobs created [c]	1	1
# of direct jobs safeguarded [c]	1	1

# of direct jobs lost	0	0

[a] *The added value or the number of items already achieved to date.*

[b] *Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve in the future (i.e. expectations within the next 3 years following the end of the project).*

[c] *"Direct jobs" means jobs within the partner involved. Research posts are to be excluded from the jobs calculation*

 # = number of ...

I confirm the information contained in part 3 of this Technological Implementation Plan and I certify that these are our exploitation intentions

Signature: **Name: Bjørn Axel Gran**

Date: January 24, 2003

insert correct date !

CONTRACT NUMBER:	**IST-2000-25031**
PARTNER's NAME:	**Norsk Regnesentral (NR)**

CONTACT PERSON:

Name	Demissie B. Aredo
Position/Title	Researcher
Organisation	Norsk Regnesentral
Address	P. O. Box 114 Blindern, 0314 Oslo, NORWAY
Telephone	+47 22 85 25 00
Fax	+47 22 69 76 60
E-mail	

Number, TITLE AND BRIEF DESCRIPTION OF MAIN RESULTS

1	*CORAS Framework*
2	*CORAS methodology for Model-based Risk Assessment (MBRA)*
3	*UML profile for Security Assessment*
4	*Repository of Reusable Elements*
5	*CORAS Platform*
6	*XML format for representation of Risk Assessment*
7	*Vulnerability and Threat Management Component*

FOR EACH MAIN RESULT:

TIMETABLE OF THE USE AND DISSEMINATION ACTIVITIES WITHIN THE NEXT 3 YEARS AFTER THE END OF THE PROJECT

Mention the use and dissemination related activities, the main associated partners, the related milestones and give an indicative timescale		
Activity	**Brief description of the activity, including main milestones and deliverables (and how it relates to data in sections 2.2 and 3.2).**	**Timescale (months)**

Consultancy	NR is a research and development institute working on project targeting a broad range of industrial, commercial and public service organisations in the national as well as the international markets. Our R&D projects range from basic research projects for developing basic knowledge platform to applied research for developing leading-edge solutions and to consultancy in the areas of ICT and Mathematical-statistical analysis. The results from the CORAS project, and the experiences gained through the project will be used for future research projects.	

FORESEEN COLLABORATIONS WITH OTHER ENTITIES

Please tick appropriate boxes (✓) corresponding to your most probable follow-up.

R&D	Further research or development	✓	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	☐
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing agreement/Franchising	☐	**INFO**	Information exchange, training	☐
JV	Joint venture	☐	**CONS**	Available for consultancy	✓
			Other	(please specify)	☐

3.2: Quantified data for each partner's main result

Items	**Currently achieved quantity** [a]	**Estimated future quantity** [b]
Economic impacts (in EURO)		
# of licenses issued (within EU)	0	0
# of licenses issued (outside EU)	0	0
Total value of licenses (in EURO)	0	0
# of entrepreneurial actions (start-up company, joint ventures…)	0	0
# of direct jobs created [c]	0	0
# of direct jobs safeguarded [c]	0	0
# of direct jobs lost	0	0

[a] *The added value or the number of items already achieved to date.*

[b] *Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve in the future (i.e. expectations within the next 3 years following the end of the project).*

[c] *"Direct jobs" means jobs within the partner involved. Research posts are to be excluded from the jobs calculation*

 # = number of ...

I confirm the information contained in part 3 of this Technological Implementation Plan and I certify that these are our exploitation intentions

Signature: **Name: Demissie B. Aredo**

Date: January 24, 2003

CONTRACT NUMBER:	**IST-2000-25031**
PARTNER's NAME:	**SINTEF**

CONTACT PERSON:

Name	Ketil Stølen
Position/Title	Senior Scientist
Organisation	SINTEF
Address	P.O.Box 124 Blindern, N-0314 Oslo, Norway
Telephone	+47 22067897
Fax	+47 22067350
E-mail	ketil.stoelen@sintef.no

Number, TITLE AND BRIEF DESCRIPTION OF MAIN RESULTS

1	CORAS Framework
2	*CORAS methodology for Model-based Risk Assessment (MBRA)*
3	UML profile for Security Assessment
4	Repository of Reusable Elements
5	CORAS Platform
6	XML format for representation of Risk Assessment
7	Vulnerability and Threat Management Component

FOR EACH MAIN RESULT:

TIMETABLE OF THE USE AND DISSEMINATION ACTIVITIES WITHIN THE NEXT 3 YEARS AFTER THE END OF THE PROJECT

Mention the use and dissemination related activities, the main associated partners, the related milestones and give an indicative timescale		
Activity	**Brief description of the activity, including main milestones and deliverables (and how it relates to data in sections 2.2 and 3.2).**	**Timescale (months)**
Further development within industrial projects	The CORAS results will be highly relevant to SINTEF partners within the commercial and public sectors. In particular, SINTEF has a close collaboration with the Norwegian Army that will benefit from the CORAS results. (Results 1-7)	**Ongoing**
Further research and development within the SARDAS project	SARDAS (15295/431) is an R&D project funded by the Research Council of Norway under the Basic ICT Research programme. Full title: Securing availability by robust design, assessment and specification (Results 1-7)	**Runs from 2003 until 2007**
Further research and development within the SECURIS project	SECURIS (152839/220) is an R&D project funded by the Research Council of Norway as a Competence Project with User-Involvement Full title: Model-driven development and analysis of secure information systems (Results 1-7)	**Runs from 2003 until 2007**
Further research and development within the iTrust project	iTrust (IST-2001-34910) is a 5th Framework EU project under the User-Friendly Information Society (IST) programme Full title: Working group on trust management in dynamic open systems (Results 1-7)	**Runs from 2002 until 2005**
MSc and PhD theses	CORAS R&D results will be further developed by several MSc and PhD students (Results 1-7)	**Ongoing**

Courses at the University of Oslo	Personnel from SINTEF are involved in teaching two master-level courses at the University of Oslo: (1) Unassailable IT systems, and (2) Modelling with Objects. (Results 2 & 3)	**Annually**

FORESEEN COLLABORATIONS WITH OTHER ENTITIES

Please tick appropriate boxes (✓) corresponding to your most probable follow-up.

R&D	Further research or development	☐ ✓	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	☐
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing agreement/Franchising	☐	**INFO**	Information exchange, training	☐ ✓
JV	Joint venture	☐	**CONS**	Available for consultancy	☐ ✓
			Other	(please specify)	☐

3.2: Quantified data for each partner's main result

Items	**Currently achieved quantity** [a]	**Estimated future quantity** [b]
Economic impacts (in EURO)	?	?
# of licenses issued (within EU)	0	0
# of licenses issued (outside EU)	0	0
Total value of licenses (in EURO)	0	0
# of entrepreneurial actions (start-up company, joint ventures…)	0	0
# of direct jobs created [c]	0	0
# of direct jobs safeguarded [c]	0	0
# of direct jobs lost	0	0

[a] *The added value or the number of items already achieved to date.*

[b] *Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve in the future (i.e. expectations within the next 3 years following the end of the project).*

[c] *"Direct jobs" means jobs within the partner involved. Research posts are to be excluded from the jobs calculation*

 # = number of ...

I confirm the information contained in part 3 of this Technological Implementation Plan and I certify that these are our exploitation intentions

Signature: **Name: Ketil Stølen**

Date: January 24, 2003

insert correct date !

CONTRACT NUMBER:	**IST-2000-25031**
PARTNER's NAME:	**Norwegian Centre for Telemedicine – University Hospital North Norway**

CONTACT PERSON:

Name	Eva Skipenes
Position/Title	Security Adviser
Organisation	NST/UNN
Address	P.O.Box 35, N-9038, Norway
Telephone	+47 77 75 40 00
Fax	+47 77 75 40 98
E-mail	eva.skipenes@telemed.no

Number, TITLE AND BRIEF DESCRIPTION OF MAIN RESULT(S)

1	CORAS Framework
2	*CORAS methodology for Model-based Risk Assessment (MBRA)*
3	UML profile for Security Assessment
4	Repository of Reusable Elements
5	CORAS Platform
6	XML format for representation of Risk Assessment
7	Vulnerability and Threat Management Component

FOR EACH MAIN RESULT:

TIMETABLE OF THE USE AND DISSEMINATION ACTIVITIES WITHIN THE NEXT 3 YEARS AFTER THE END OF THE PROJECT

Mention the use and dissemination related activities, the main associated partners, the related milestones and give an indicative timescale		
Activity	**Brief description of the activity, including main milestones and deliverables (and how it relates to data in sections 2.2 and 3.2).**	**Timescale (months)**

Workshop/tutorial for developers of IT systems for the health care sector in Norway/the Nordic countries	NST/UNN plans to invite developers of IT systems for the health care sector in Norway and other Nordic countries to a workshop/tutorial on risk assessment using the CORAS model-based risk assessment framework, in cooperation with other CORAS partners (IFE and Telenor). (Results 1-7)	**6 – 12 months after the end of the project**
Consultancy	NST/UNN will be available for consultancy for health care related companies and organizations that want assistance in performing model-based risk assessment. (Results 1-7)	**Ongoing**

FORESEEN COLLABORATIONS WITH OTHER ENTITIES

Please tick appropriate boxes (✓) corresponding to your most probable follow-up.

R&D	Further research or development	☐	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	☐
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing agreement/Franchising	☐	**INFO**	Information exchange, training	☑
JV	Joint venture	☐	**CONS**	Available for consultancy	☑
			Other	(Please specify)	☐

3.2: Quantified data for each partner's main result

Items	**Currently achieved quantity** [a]	**Estimated future quantity** [b]
Economic impacts (in EURO)	?	?
# of licenses issued (within EU)	0	0
# of licenses issued (outside EU)	0	0
Total value of licenses (in EURO)	0	0
# of entrepreneurial actions (start-up company, joint ventures…)	0	0
# of direct jobs created [c]	0	0
# of direct jobs safeguarded [c]	0	0
# of direct jobs lost	0	0

[a] *The added value or the number of items already achieved to date.*

[b] *Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve in the future (i.e. expectations within the next 3 years following the end of the project).*

[c] *"Direct jobs" means jobs within the partner involved. Research posts are to be excluded from the jobs calculation*

 # = number of ...

I confirm the information contained in part 3 of this Technological Implementation Plan and I certify that these are our exploitation intentions

Signature: **Name: Eva Skipenes**

Date: January 21, 2003

insert correct date !

CONTRACT NUMBER:	**IST-2000-25031**
PARTNER's NAME:	**CCLRC - RAL**

CONTACT PERSON:

Name	Theo Dimitrakos
Position/Title	Senior Scientist
Organisation	Central Laboratory of the Research Councils – Rutherford Appleton Lab.
Address	Rutherford Appleton Laboratory, OX 11 0QX, UK
Telephone	+44 1235 446387
Fax	+44 1235 445381
E-mail	t.dimitrakos@rl.ac.uk

Number, TITLE AND BRIEF DESCRIPTION OF MAIN RESULT(S)

1	The CORAS Framework
2	*CORAS methodology for Model-based Risk Assessment (MBRA)*
3	UML profile for Security Assessment
4	Repository of Reusable Elements
5	CORAS Platform
6	XML format for representation of Risk Assessment
7	Vulnerability and Threat Management Component

FOR EACH MAIN RESULT:

TIMETABLE OF THE USE AND DISSEMINATION ACTIVITIES WITHIN THE NEXT 3 YEARS AFTER THE END OF THE PROJECT

Mention the use and dissemination related activities, the main associated partners, the related milestones and give an indicative timescale		
Activity	**Brief description of the activity, including main milestones and deliverables (and how it relates to data in sections 2.2 and 3.2).**	**Timescale (months)**

Consultancy	CCLRC owns and operates the Rutherford Appleton Laboratory (RAL) in Oxfordshire, the Daresbury Laboratory (DL) in Cheshire and the Chilbolton Facility in Hampshire. These institutions support the research community by providing access to advanced facilities and an extensive scientific and technical expertise. CLRC Facilities include ISIS, the world's most powerful pulsed neutron and muon source - for research into the atomic structure of materials; the Synchrotron Radiation Source, the UK's brightest source of ultraviolet light and X-rays – for research in materials and life sciences; the Central Laser Facility, high-power state-of-the-art laser facilities; satellite and ground based instrumentation, testing and data analysis for earth observation, astronomy and planetary science; the UK e-Science Grid Support Centre, e-Science support of the UK particle physics research programmes at CERN and elsewhere; computing, networking services and user support; etc. A main objective of the Business and Information Technology Department of CLRC is to provide CLRC and the UK with effective business and information technology through delivery of innovative systems and services. The knowledge gained in CORAS and CORAS R&D results will be used for consultancy offered by BITD staff *within CLRC* leading to improvements in the operation and management of CLRC facilities. (Results 1-7)	**Ongoing**
Further research and development within the iTrust project	iTrust (IST-2001-34910) is a 5th Framework EU project under the User-Friendly Information Society (IST) programme Full title: Working group on trust management in dynamic open systems (Results 1-7)	**Runs from 2002 until 2005**
MSc and PhD theses	CCLRC staffs are often co-supervising MSc and PhD students of UK Universities. CORAS R&D results will be further developed by several MSc and PhD students (Results 1-7)	**Ongoing**

University Courses	CCLRC staffs are involved in teaching MSc courses on Critical Systems, Web Technologies and Software Engineering of Internet Applications at various UK Universities (such as Imperial College, King's College London, and Oxford Brookes College). CORAS R&D results provide useful input for these courses. (Results 2,3,6)	**Annually**
Industrial Training	CCLRC staffs are involved in teaching Industrial Training courses on site and at UK Universities (such as Imperial College and King's College London). CORAS R&D results provide useful input for these courses. (Results 2,3,6)	**Periodically**

FORESEEN COLLABORATIONS WITH OTHER ENTITIES

Please tick appropriate boxes (✓) corresponding to your most probable follow-up.

R&D	Further research or development	✓	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	☐
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing agreement/Franchising	☐	**INFO**	Information exchange, training	✓
JV	Joint venture	☐	**CONS**	Available for consultancy	✓
			Other	(please specify)	☐

3.2: Quantified data for each partner's main result

Items	**Currently achieved quantity** [a]	**Estimated future quantity** [b]
Economic impacts (in EURO)	0	?
# of licenses issued (within EU)	0	0
# of licenses issued (outside EU)	0	0
Total value of licenses (in EURO)	0	0
# of entrepreneurial actions (start-up company, joint ventures…)	0	0
# of direct jobs created [c]	0	?
# of direct jobs safeguarded [c]	0	?
# of direct jobs lost	0	0

[a] *The added value or the number of items already achieved to date.*

[b] *Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve in the future (i.e. expectations within the next 3 years following the end of the project).*

[c] *"Direct jobs" means jobs within the partner involved. Research posts are to be excluded from the jobs calculation*

 # = number of ...

I confirm the information contained in part 3 of this Technological Implementation Plan and I certify that these are our exploitation intentions

Signature: **Name: Theo Dimitrakos**

Date: Feb. 13, 2003

insert correct date !

CONTRACT NUMBER:	**IST-2000-25031**
PARTNER's NAME:	**Queen Mary and Westfield College (QMW)**

CONTACT PERSON:

Name	Eric Scharf
Position/Title	Dr.
Organisation	Dept. of Electronic Engineering
Address	Queen Mary, University of London, London E1 4NS, United Kingdom.
Telephone	+44 2078825530
Fax	+44 2078827997
E-mail	e.m.scharf@elec.qmul.ac.uk

Number, TITLE AND BRIEF DESCRIPTION OF MAIN RESULT

1	The CORAS Framework
2	CORAS methodology for Model-based Risk Assessment (MBRA)
3	UML profile for Security Assessment
4	Repository of Reusable Elements
5	CORAS Platform
6	XML format for representation of Risk Assessment
7	Vulnerability and Threat Management Component

FOR EACH MAIN RESULT:

TIMETABLE OF THE USE AND DISSEMINATION ACTIVITIES WITHIN THE NEXT 3 YEARS AFTER THE END OF THE PROJECT

Mention the use and dissemination related activities, the main associated partners, the related milestones and give an indicative timescale		
Activity	**Brief description of the activity, including main milestones and deliverables (and how it relates to data in sections 2.2 and 3.2).**	**Timescale (months)**

Undergraduate and M.Sc. courses	In view of the importance of security topics the educational market in this area is potentially very large. QMW currently teaches courses modules dealing with security issues in the telecommunications domain. The CORAS framework will be used to illustrate and demonstrate these issues. This will be the first known application of a security assessment framework in the educational environment. The courses where the CORAS framework is of particular interest are the Undergraduate and Graduate courses on Internet Engineering and E-Commerce Engineering and in the intercollegiate courses offered to industry. One of these intercollegiate courses is the Post Graduate MSc course for British Telecom, which consists of several two-week long modules. BT course modules are often given to between 50 to 100 students. (Result 1, 2 and 5)	**3**
Research projects	As an academic institution, one of the benefits of CORAS will be the publication of research papers in international journals and conferences. Publications lead to further work and ideas for research projects. These projects are suited for research leading to a research degree (e.g. PhD.) CORAS will be used as an assessment tool for a PhD project on secure users groups. This project will use intelligent agents to implement algorithms and reasoning process for closed user groups. It is envisaged that CORAS can also be used for other PhD and MSc research projects at QMW. (Result 5).	

FORESEEN COLLABORATIONS WITH OTHER ENTITIES

Please tick appropriate boxes (✓) corresponding to your most probable follow-up.

R&D	Further research or development	✓	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	☐
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing agreement/Franchising	☐	**INFO**	Information exchange, training	✓
JV	Joint venture	☐	**CONS**	Available for consultancy	
			Other	(please specify)	☐

3.2: Quantified data for each partner's main result

Items	Currently achieved quantity [a]	Estimated future quantity [b]
Economic impacts (in EURO)	0	?
# of licenses issued (within EU)	0	0
# of licenses issued (outside EU)	0	0
Total value of licenses (in EURO)	0	0
# of entrepreneurial actions (start-up company, joint ventures…)	0	0
# of direct jobs created [c]	0	?
# of direct jobs safeguarded [c]	0	?
# of direct jobs lost	0	0

[a] *The added value or the number of items already achieved to date.*

[b] *Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve in the future (i.e. expectations within the next 3 years following the end of the project).*

[c] *"Direct jobs" means jobs within the partner involved. Research posts are to be excluded from the jobs calculation*

 # = number of ...

I confirm the information contained in part 3 of this Technological Implementation Plan and I certify that these are our exploitation intentions

Signature: **Name: Dr. Eric Scharf**

Date: Feb. 13, 2003

CONTRACT NUMBER:	**IST-2000-25031**
PARTNER's NAME:	**Research Academic Computer Technology Institute (CTI)**

CONTACT PERSON:

Name	Sotiris Nikoletseas
Position/Title	Manager of Research Unit 1
Organisation	Research Academic Computer Technology Institute
Address	61 Riga Feraiou Str., Patras, Greece
Telephone	+30-2610-960324
Fax	+30-2610-960442
E-mail	nikole@cti.gr

Number, TITLE AND BRIEF DESCRIPTION OF MAIN RESULTS

1	The CORAS Framework
2	*CORAS methodology for Model-based Risk Assessment (MBRA)*
3	UML profile for Security Assessment
4	Repository of Reusable Elements
5	CORAS Platform
6	XML format for representation of Risk Assessment
7	Vulnerability and Threat Management Component

FOR EACH MAIN RESULT:

TIMETABLE OF THE USE AND DISSEMINATION ACTIVITIES WITHIN THE NEXT 3 YEARS AFTER THE END OF THE PROJECT

Mention the use and dissemination related activities, the main associated partners, the related milestones and give an indicative timescale		
Activity	**Brief description of the activity, including main milestones and deliverables (and how it relates to data in sections 2.2 and 3.2).**	**Timescale (months)**

Applying CORAS on a lottery system	There is a CTI project on designing and building information systems for the support of games of luck and fixed odds. The system under analysis is a lottery system that supports football fixed odds games. The subsystem to be analysed by CTI was responsible for ensuring the integrity of the coupon files. During the risk assessment CTI followed the CORAS framework as described in the CORAS technical deliverables. Work on this project is still ongoing as the system underwent some modifications and it is still under testing. (Result 1)	**3**
Consultancy	Since 1995 CTI serves as technical and research consultant to Greek ministries and parts of the Greek public sector in the areas of information and communication technologies. CTI has collaborated with the Ministry of National Education and Religious Affairs, the Ministry of Health and Welfare, the Ministry of Mercantile Marine and the Ministry of National Economy, as well as the Athens Stock Exchange and the Greek Parliament. For instance, CTI collaborated with the University of Ioannina and the Hellenic Telecommunications Organisation on planning and establishing the Centre of Telematics of Western Greece, Epirus and Ionian Islands. CTI could extend its consulting services by incorporating the CORAS framework into them. But CTI does not have the expertise and tools on the CORAS framework that other CORAS partners have, so it is envisioned that such consulting services can only be provided in collaboration with other partners. (Results 1-7)	

FORESEEN COLLABORATIONS WITH OTHER ENTITIES

Please tick appropriate boxes (✓) corresponding to your most probable follow-up.

R&D	Further research or development	☐	**FIN**	Financial support	☐
LIC	Licence agreement	☐	**VC**	Venture capital/spin-off funding	☐
MAN	Manufacturing agreement	☐	**PPP**	Private-public partnership	☐
MKT	Marketing agreement/Franchising	☐	**INFO**	Information exchange, training	☐
JV	Joint venture	☐	**CONS**	Available for consultancy	✓
			Other	(please specify)	☐

3.2: Quantified data for each partner's main result

Items	**Currently achieved quantity** [a]	**Estimated future quantity** [b]
Economic impacts (in EURO)	21000 (Result 1)	?
# of licenses issued (within EU)	0	0

# of licenses issued (outside EU)	0	0
Total value of licenses (in EURO)	0	0
# of entrepreneurial actions (start-up company, joint ventures…)	0	0
# of direct jobs created [c]	0	?
# of direct jobs safeguarded [c]	3 (Result 1)	?
# of direct jobs lost	0	0

[a] *The added value or the number of items already achieved to date.*

[b] *Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve in the future (i.e. expectations within the next 3 years following the end of the project).*

[c] *"Direct jobs" means jobs within the partner involved. Research posts are to be excluded from the jobs calculation*

 # = number of ...

I confirm the information contained in part 3 of this Technological Implementation Plan and I certify that these are our exploitation intentions

Signature: **Name: Sotiris Nikoletseas**

Date: January 24, 2003

insert correct date !

Appendix

Technical deliverables

Deliverables on risk management:

D2.1 Technical report reviewing existing Risk Analysis methodology and techniques, with evaluation of their applicability to security critical systems

D2.2 Preliminary report on risk analysis methodology

D2.3 Preliminary report on templates and guidelines

D2.4 Technical report providing templates and/or guidelines on how to adapt and extend existing risk analysis methodology for security critical systems

D2.5 Evaluation report on effectiveness of guidelines

Deliverables on modelling and specification

D3.1 Report on the state-of-the-art in the area of object-oriented description methods and commercial products that are employed in security modelling

D3.2 Report describing the resulting RM-ODP inspired modelling framework with specialised support for security and risk analysis

D3.3 Report describing structure for storing and maintaining standard library components

D3.4 Report outlining scenario-driven design tactics (based on the preliminary trial descriptions) in order to exemplify the best use of modelling assemblies (rules, patterns, standard library components) in specifying security policies.

D3.5 Report presenting patterns and rules for how risk analysis within one part of a model can be exploited to simplify, guide or improve the effectiveness of risk analysis within another part of the model or within another viewpoint. Particular emphasis will be given on the description of procedures to assure the consistency of security handling within the modelling framework.

D3.6 Libraries of standard modelling elements expressed in object-oriented and other for this purpose selected specification methods

D3.7 Revision of D3.2-6 after theoretical analysis and practical experience in integration and application trials.

D3.8 Evaluation report on the effectiveness of work package 3.

Deliverables on methods, tools and techniques integration

D4.1 Initial "CORAS-process guideline"

D4.2 Evaluation of different tool chains

D4.3 Formats for integration

D4.4 Revised CORAS toolset, guidelines and full documentation

D4.5 Revision of D4.1 and 4.3 based on further experiences

D4.6 Evaluation report on the integration activities

Deliverables on field trials in telemedicine and e-commerce

D5.1 Descriptions of applications and trials

D5.2 Risk analysis report on the E-commerce Authentication mechanism documenting the identified and analysed risks.

D5.3, D5.10, D5.14 First, second, and third CORAS E-commerce trial.

D5.4, D5.6 First and second Risk Analysis of ATTRACT

D5.5, D5.8, D5.12 First, second and third Telemedicine Assessment Report.

D5.7, D5.11 First and second Risk Analysis of Tele-Cardiology

D5.9 Risk Analysis report on the E-commerce Secure Payment mechanism

D5.13 Risk Analysis report on the E-Commerce Agents mechanism

D5.15 Trials results and assessments.

Deliverables on Implementation, Dissemination and Use Plan

D7.3 Dissemination and Use Plan (DUP)

D7.4 Technology Implementation Plan (TIP)