information society technologies

CORAS

Risk Assessment of Security Critical Systems

Project Number:	IST-2000-25031
Project Title:	CORAS
Deliverable Security*:	RE
CEC Deliverable Number:	D7.6
Contractual Delivery Date:	30/06/2003
Actual Delivery Date:	30/08/2003
Deliverable Title:	**Technology Implementation Plan, Final Version**
Version:	03.043 WP7 Act 7.1 D7.6 V1.0
Principal WP Contributor:	WP7
Deliverable Type:**	R
Authors:	Demissie B. Aredo (NR)
Contributors:	Siv H. Houmb, Eirik M. Knudsen, Tony Price, Erik-Dagfinn Wisløff (Telenor); Dimitris Raptis (Intracom); Gustav Dahl, Bjørn Axel Gran, Atoosa P.J. Thunem (IFE); Mass S. Lund, Ketil Stølen (Sintef); Eva Skipenes (NCT-UNN); Theo Dimitrakos (CCLRC); Eric Scharf (QMW); Sotiris Nikoletseas (CTI); Michael Loupis, Katerina Papadaki (Solinet); Manolis Tsiknakis (FORTH)

*** 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 final Technical Implementation Plan (TIP) of the CORAS project, at the end of the 30-month project. The TIP describes the 7 results of the project: (1): the CORAS framework; (2) the CORAS methodology for model-based risk assessment (MBRA); (3) the CORAS UML profile for security assessment; (4) the CORAS library of reusable experience packages; (5) the CORAS integration platform; (6) the CORAS XML mark-up for security assessment; and (7) the CORAS vulnerability assessment component. The TIP also documents the partners' exploitation intentions.

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

Executive summary

This document, contractually known as deliverable D7.6, is the final version of Technical Implementation Plan (TIP) for the CORAS project. The TIP describes the major results of the project, and how they will be exploited after the end of the project. The TIP has evolved during the course of the project through two major iterations: the first version was submitted as deliverable D7.3 in August 2002, and the second as D7.4 in February 2003.

The TIP comprises three major parts. Part I provides a brief overview of the CORAS project objectives and its results:

1 The CORAS framework

2 The CORAS methodology for model-based risk assessment (MBRA)

3 The CORAS UML profile for security assessment

4 The CORAS library of reusable experience packages

5 The CORAS integration platform

6 The CORAS XML mark-up for security assessment

7 The CORAS vulnerability assessment component

Part II describes the main results achieved in the project. Part III describes the plan of individual CORAS partners for their future exploitation.

All CORAS results are freely available. In particular, the source-code is available as open source on a GNU Lesser General Public License.

All CORAS partners have the intention of exploiting part of the project's results within the context of their present academic/commercial/geographical organisations, and these intentions are explained in Part III.

In addition to the TIP, the consortium has produced a business plan approach. This extra document is meant to be read as a supplement in conjunction with the TIP and may be taken as preliminary reading about a commercial approach for any potential investor interested in the exploitation of CORAS products and services.

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

a. Original research objectives

The CORAS project was intended 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 main objectives of the CORAS project were:

- 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. Deliverables achieved

The administrative and research activities in the CORAS project and their results have been documented and reported to interested groups, including partners, the EU Commission, potential users and researchers 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 and a project brochure.) 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 has achieved a particular solution for model-based risk assessment (MBRA) for security-critical systems. It also addresses issues related to the development environment for assisting the instantiations of the MBRA beyond the project period.

It identifies 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 very relevant to all security-critical systems, especially to telemedicine and e-commerce related applications. They are customisable and hence their potential is now available to potential investors.

The main results of the CORAS project put the partners in a mutually complementary relationship. The commercial partners are fully convinced of the merits of the results that have been achieved through their requirements and participation, and some will proceed to integrate the resulting CORAS framework into their development process and exploit it internally. The research and development partners are working with standardisation bodies and major national institutions to exploit the CORAS results. They are also putting their efforts behind necessary add-ons for enforcing policies at the administrative level through appropriate further tools.

Finally, the educational partners plan to introduce the CORAS methodology into their curriculum.

d. Broad dissemination and use intentions for the expected outputs

As is typical of EU projects, the competences and interests of the partners in the CORAS consortium vary from commercial partners to research and development partners to educational partners. This strength of CORAS will bear its fruit during the post-project exploitation phase, when the partners will all concentrate on those parts of the project results relating to their specific activity domains and exploit their relevant elements within their contextual possibilities. For example, academic members will incorporate the CORAS platform into their appropriate teaching curricula, commercial partners will apply part/all of the CORAS risk assessment process in their own risk management systems, while research establishments will begin to sew the CORAS seeds in new programmes of CORAS-derived ongoing research.

The CORAS project has succeeded in achieving certain technical novelties and breakthroughs, and it is in these areas in particular, where the present commercial exploitation and ongoing research opportunities will make the most significant impact.

Due to the partner group interests and resultant project objectives, CORAS centred its trial activities in the areas of telemedicine and e-commerce, and so the results will have an immediate applicability in these two fields. However, the CORAS platform and associated tools are fully flexible, and will be capable of adaptation to any commercial context needing the implementation of risk management (insurance, oil, banking, to name some of the more obvious examples). Indeed, most medium to large-sized companies are already potential customers for consumer-friendly, cost-saving, security-enhancing, risk-limiting risk management. Full details of the project's broadly-based dissemination programme and achievements are available in deliverable 6.3.

2 Overview of CORAS results

No.	Self-descriptive title of the result	Category A, B or C[1]	Partner(s) owning the result(s) (referring in particular to specific patents, copyrights, etc.) & involved in their further use
1	*The CORAS framework*	A	All partners
2	*The CORAS methodology for model-based risk assessment (MBRA)*	A	All partners
3	*The CORAS UML profile for security assessment*	A	All partners
4	*The CORAS library of reusable experience packages*	A	All partners
5	*The CORAS integration platform*	A	All partners
6	*The CORAS XML mark-up for security assessment*	A	All partners
7	*The CORAS vulnerability assessment component*	A	All partners

[1] * 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)	0	1
# of process innovations (commercial)	0	1
# of new services (commercial)	0	0
# of new services (public)	0	0
# of new methods (academic)	1	1
# of scientific breakthrough	0	0
# of technical standards to which this project has contributed	2	1
# of EU regulations/directives to which this project has contributed	0	0
# of international regulations to which this project has contributed	0	0
# of PhDs generated by the project	0	3
# of grantees/trainees including trans-national exchange of personnel	0	0

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

3.1 Comment on European Interest

"***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[2]:

- 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

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

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.

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 CORAS.

3.2 Community added value and contribution to EU policies

a. European added value

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 contributes 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 enable the realisation of long promised changes in our way of working and living. There will be many changes including in the area of tele working, telemedicine and advanced electronic commerce. Preparing the infrastructure for electronic commerce is a particularly important EU policy, which will greatly benefit from improved risk assessment 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 conducting the co-ordination of development activities, as this cannot be initiated and driven from a single country.

b. Contribution to developing S&T co-operation at international level. The fact that a research and technological development project like CORAS could contribute and add value to various other projects throughout the IST programme was appreciated, early on by the CORAS consortium. This motivated the establishment of a workpackage, namely WP8, dedicated to the investigation, planning and coordination of synergies with other projects in targeted areas including health, dependability, security and trust management.

One objective for the establishment of synergies with key actors in the market and other projects within the targeted areas of the IST programme mentioned above was to facilitate the take up of CORAS results. Another objective was to contribute to the development of the CORAS framework by either providing a wider user base for eliciting requirements and evaluating results or offering scientific expert advise in areas complementing the security assessment work undertaken in the context of the CORAS project.

The impact of synergies between CORAS and other RTD or take-up projects can be understood as follows:

- Synergy with other projects enables CORAS to achieve a critical mass (e.g., in technology, standardisation, and regulatory issues) through which it may be able to influence European political and regulatory bodies and/or lead to the creation of international standardised platforms utilising model based risk management.

- Synergy with projects focusing on complementary aspects of trust and confidence building in information systems, such as social, enterprise and legal aspects, or other aspects of dependability (e.g. safety, reliability, timelines, maintainability, etc.), enrich the know-how of the consortium. Moreover, it further our understanding of the problems at hand, and result in improvements of the quality, effectiveness and exploitation potential of the CORAS results. Such co-operation is an increasing prerequisite for capturing a global market.

- Synergy with projects which include complementary technical skills, such as CASE-tool providers, major software and telecommunications vendors, may help to improve return of investment in the projects through sharing results or fusing our implementation and usage plans.

The continuous efforts of the CORAS consortium resulted in the initiation of two initiatives, one in the area of *e-health*, instigated by NCT, and one in the area of *trust management*, instigated by CCLRC/RAL. Furthermore, from early on, CORAS actively participated in DEPPY - "The European Dependability Initiative". Through these activities WP8 ensured that CORAS results are taken up by other projects within the IST programme and lead to the definition of further integrated research.

CORAS contributions to the above include the CORAS methodology for risk analysis and the CORAS framework supported by computerised tools, competence on risk management, risk assessment, security and modelling. The additional understanding obtained through these synergies has helped

CORAS to develop a better framework and methodology that is more likely to solve real-life problems.

Impact of clustering in the health domain

The former of the two initiatives instigated by CORAS focused on the establishment of a thematic network on fundamental information security issues underpinning information and telecommunication systems for e-Health and telemedicine, and was based on a synergy between the CORAS, RESHEN and HARP projects. Over the time the close synergy between these three projects expanded to include C-CARE, SECRETS, DIGISEC, and PKI-Challenge. In order to sustain a longer-term synergistic plan, this initiative resulted in a proposal for establishing a thematic network under the acronym SEC-Health. An initial attempt to secure funding for this thematic network within the 5th Framework Programme was unsuccessful, and the potential of a second attempt in the context of the 6th Framework Programme has been assessed.

Impact of clustering in the security and trust domain

The latter of the two initiatives instigated by CORAS has now resulted in a well established thematic network, named *"iTrust: Working Group on Trust Management in Dynamic Open Systems"*. This thematic network is first in Europe to explicitly address this research and technological development area in the context of the Future and Emerging Technologies activity of the IST programme, funded under contract IST-2001-34910. CORAS has been one of the four founding projects of iTrust thematic network, and the only focusing on the interplay between risk assessment, security policy definition and enforcement, and trust establishment in dynamic, open and scalable distributed systems. The other three contributing projects are SECURE (IST-2001-32486) focusing on computational trust models, ALFEBiiTE (IST-1999-10298) focusing on formal treatment of models for trust, deception and fraud in virtual communities, and iCities (IST-1999-10298) focusing on dynamics of cluster formation.

iTrust working group is also organising an annual International Conference on Trust Management and working group workshops every six months. The first workshop (in Scotland) and international conference (in Crete) attracted in total an audience of 120 researchers while the proceedings of the first conference were published by the Lecture Notes in Computer Science series of Springer Verlang. Through these activities, experience from the CORAS approach and framework is reaching a vibrant community of researchers in academia and industry in Europe, USA, Canada and Australia.[3]

Impact of clustering in the dependability domain

From the early stages of the project, CORAS actively participated in in DEPPY - "The European Dependability Initiative", which operates as a cluster of fifteen IST projects across several action lines. Through continuous and proactive participation in DEPPY activities, it has been ensured that CORAS results are taken up by other projects within the IST programme and lead to the definition of further integrated research. Furthermore, CORAS input on the future of dependability research and technological development in Europe was also provided through contributions to the AMSD roadmap project.

[3] The iTrust network includes affiliate members in the USA, namely IBM Watson, the Institute of Advanced Commerce, in Canada, namely the National Research Council of Canada, and in Australia, namely the Distributed Systems Technology Center.

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[4]:

- 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 aids in solving the aforementioned problem. Its structured approach in modelling, specifying and risk-analysing security critical systems improves the implementation and maintenance of secure systems and thus, strengthens the security assurance of large systems and reinforces 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 leads to the creation of the desired

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

secure-feeling that a modern Information Society is pursuing.

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 offer 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[5]

	I	II	
	SCALE OF EXPECTED IMPACT OVER THE NEXT 10 YEARS[6]	**Others**	
EU Policy Goals	-1 0 1 2 3	**Not applicable to project**	**Project Impact too difficult to estimate**
1. Improved sustainable economic development and growth, competitiveness	1	□	□
2. Improved employment	1	□	□
3. Improved quality of life and health and safety	3	□	□
4. Improved education	1	□	□
5. Improved preservation and enhancement of the environment	0	□	☑

[5] 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.

[6] 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

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

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	1	1
- International markets	1	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	2
b) Improved food, nutrition	0	0
c) Improved safety (incl. consumers and workers safety)	0	2
d) Improved quality of life for the elderly and disabled	0	2
e) Improved life expectancy	0	2
f) Improved working conditions	0	2
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	**After Project End**
	-1 0 1 2 3	-1 0 1 2 3
a) Improved learning processes including lifelong learning	0	0
b) Development of new university curricula	1	2

5. Preservation and enhancement of the environment	**Scale of Expected Impacts over the next 10 years** (2)	
	By Project End	**After Project End**
	-1 0 1 2 3	-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	**After Project End**
	-1 0 1 2 3	-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	1	0
d) Enhance skills of RTD staff	2	1
e) Transfer expertise/know-how/technology	2	2
f) Improved access to knowledge-based networks	1	1
g) Identifying appropriate partners and expertise	0	1
h) Develop international S&T co-operation	3	2
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	0	0
b) Contribution to EU policy implementation	0	2

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: August 30, 2003 **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	Erik Dagfinn Wisløff
Position	Senior Engineer
Organisation	Telenor Communication II AS
Address	Snarøyveien 30, 1331 Fornebu
Telephone	+47 909 50 223
Fax	N/A
E-mail	erik-dagfinn.wisloff@telenor.com
URL	http://www.telenor.com
Specific Result URL	http://sourceforge.net/projects/coras

SUMMARY

The main result of the CORAS project is the CORAS framework for model-based risk assessment of security-critical systems. The framework consists of terminology, languages for system modelling, processes for system development and risk management, methodologies for security risk analysis as well as computerised tools. 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 integration 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 assessment (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**
CORAS Deliverable	D2.4 The CORAS methodology for model-based risk assessment	PU
CORAS Deliverable	D3.7 The CORAS framework, the CORAS UML profile for security assessment, and the CORAS library of reusable experience packages	PU
CORAS Deliverable	D4.4 The CORAS toolset, guidelines and full documentation (source code)	CO
CORAS Deliverable	D4.5 The CORAS integration platform, the CORAS XML-markup for security assessment, the CORAS vulnerability assessment component	CO
CORAS Deliverable	D5.15 Trial results and assessment of the CORAS methodology	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	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)		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.	1	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

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 agreement/Franchising	√	**INFO**	Information exchange	√
JV	Joint venture	□	**CONS**	Available for consultancy	√
			Other	Standardisation	√

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

The CORAS framework is freely available. In particular, the source-code for its computerised components is available as open source on a GNU Lesser General Public License. For additional details on this, see the corresponding section in the description of Result 5.

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 II of this Technological Implementation Plan and I authorise its dissemination to assist this search for collaboration.

Signature:

Name: Tony Price

Date: August 30, 2003

Organisation: Telenor R&D

Description of Result 2

No. & TITLE OF RESULT

No.	Self-descriptive title of the result
2	*The CORAS methodology form 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	http://sourceforge.net/projects/coras

SUMMARY

The CORAS methodology for model-based risk assessment (MBRA) applies the standardised modelling technique UML to form input models to risk analysis methods that are used in a risk management process. This process is based on the standard AS/NZS 4360:1999 “Risk Management”.

The CORAS methodology for MBRA can be utilised on three abstraction levels, and for each level recommendations and guidelines are provided, as well as templates, questionnaires and supportive descriptions. The CORAS methodology for MBRA may also be understood as specialisation and further refinement of the recommendations for the CORAS risk management process, and as a refined sub-specification for the CORAS Platform. Finally, the CORAS methodology for MBRA is specialised towards assessment of security critical systems.

The CORAS methodology for MBRA has been tested and turned out successfully on telemedicine and e-commerce systems through several trials. The benefit from using the methodology 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**
CORAS Deliverable	D2.4 The CORAS methodology for model-based risk assessment	PU
CORAS Deliverable	D5.15 Trial results and assessment of the CORAS methodology	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	10
of which : number of SMEs :	1	0
of which : number of entities in third countries (outside EU) :	5	3
Targeted user audience: # of reachable people		> 100 000
# of S&T publications (referenced publications only)	2	2
# of publications addressing general public (e.g. CD-ROMs, WEB sites)	1	1
# of publications addressing decision takers / public authorities / etc.	9	5
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

The CORAS methodology for model-based risk assessment is intended to form a basis for future proposals for FP6 as well as the Norwegian Research Council.

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 agreement/Franchising	□	**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.

The CORAS framework of which this result is a major component is freely available. In particular, the source-code for its computerised components is available as open source on a GNU Lesser General Public License. For additional details on this, see the corresponding section in the Description of Result 5.

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 II of this Technological Implementation Plan and I authorise its dissemination to assist this search for collaboration.

Signature: **Name: Bjørn Axel Gran**

Date: August 30, 2003 **Organisation:** Institute for Energy Technology

Description of Result 3

No. & TITLE OF RESULT

No.	Self-descriptive title of the result
3	***The CORAS UML profile for security assessment***

Contact person for this result:

Nam	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	http://sourceforge.net/projects/coras

SUMMARY

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

- One major challenge when performing a risk assessment is to establish a common understanding of the target of evaluation, threats, vulnerabilities and risks among the stakeholders participating in the assessment. The CORAS UML profile may be understood as a UML extension providing specialised support for communication during structured brainstorming session that improves the communication ability during risk assessments. The profile makes the UML diagrams easier to understand for non-experts, and at the same time preserves the well-definedness of UML.
- Requirements to security documentation and the demands to document security issues are increasing. This raises the issue of standards for ensuring and documenting the security of IT systems. The CORAS UML profile for risk assessment has been submitted to the OMG for standardisation, and is likely to be voted on at the OMG meeting in November this year.
- Risk assessments are costly and time consuming and should not be initiated from scratch each time we assess a new or modified system. Documenting risk assessments using UML supports reuse of risk assessment documentation, both for systems that undergo maintenance and for new systems, if similar systems have been assessed earlier. The CORAS UML profile for risk assessment provides rules and constraints for risk assessment relevant system documentation.

Please categorise the result using codes from Annex 1

Subject descriptors codes	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**
CORAS Deliverable	D3.7 The CORAS framework, the CORAS UML profile for security assessment, and the CORAS library of reusable experience packages	PU
CORAS Deliverable	D5.15 Trial results and assessment of the CORAS methodology	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	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:	2	2
of which : number of SMEs :	0	0
of which : number of entities in third countries (outside EU) :	2	2
Targeted user audience: # of reachable people	0	> 100 000
# of S&T publications (referenced publications only)	3	10
# of publications addressing general public (e.g. CD-ROMs, WEB sites)	1	10
# of publications addressing decision takers / public authorities / etc.	1	10
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 agreement/Franchising	□	**INFO**	Information exchange	□
JV	Joint venture	□	**CONS**	Available for consultancy	□
			Other	Standardisation	√

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

Under the leadership of SINTEF, 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". The proposal has received positive response and was resubmitted both in May and August this year, and will probably be voted on at the OMG meeting in November.

The CORAS framework of which this result is a major component is freely available. In particular, the source-code for its computerised components is available as open source on a GNU Lesser General Public License. For additional details on this, see the corresponding section in the Description of Result 5.

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: August 30, 2003	**Organisation: SINTEF**

Description of Result 4

No. & TITLE OF RESULT

No.	Self-descriptive title of the result
4	***The CORAS Library of Reusable Experience Packages***

Contact person for this result:

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

SUMMARY

A significant part of the results of a security analysis carried out on an IT-system will typically have a certain general character. To avoid starting from scratch for every new analysis, it is important to gather these general aspects. The library of reusable experience packages captures such generic aspects in the form of e.g. UML-diagrams, table-formats, check lists, patterns and plain text.

Each experience package is decomposed into experience elements. An experience package belongs to a domain, but may inherit elements from experience packages of other domains; e.g., an experience package in the telemedicine domain may inherit elements from experience packages in the health domain and the general domain.

The experience packages are classified into constructive and supportive packages, which contain constructive and supportive elements, respectively. A supportive package documents methodological aspects like guidelines and recommendations while a constructive package provides formats and patterns for the documentation of assessment results and the assumptions on which they depend.

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**
CORAS Deliverable	D3.7 The CORAS framework, the CORAS UML profile for security assessment, and the CORAS library of reusable experience packages	PU
CORAS Deliverable	D5.15 Trial results and assessment of the CORAS methodology	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	2
of which : number of SMEs :	0	0
of which : number of entities in third countries (outside EU) :	1	1
Targeted user audience: # of reachable people	0	> 100 000
# of S&T publications (referenced publications only)	3	2
# of publications addressing general public (e.g. CD-ROMs, WEB sites)	0	10
# of publications addressing decision takers / public authorities / etc.	1	10
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 agreement/Franchising	□	**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 framework of which this result is a major component is freely available. In particular, the source-code for its computerised components is available as open source on a GNU Lesser General Public License. For additional details on this, see the corresponding section in the Description of Result 5.

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: August 30, 2003	**Organisation: SINTEF**

Description of Result 5

No. & TITLE OF RESULT

No.	Self-descriptive title of the result
5	***The CORAS integration platform***

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	http://sourceforge.net/projects/coras

SUMMARY

The CORAS integration platform is the main computerised component of the CORAS framework.

The CORAS platform is used to store the results from ongoing and completed security analyses, as well as the reusable elements and experience packages. These are stored in two separate repositories, the Assessment Repository for the analysis results, and the Reusable Elements Repository for the reusable elements. During a security analysis, reusable elements may be instantiated and become part of the security analysis results. The platform GUI provides the end-user with administrative functionality, such as creating new security analysis projects and managing the reusable elements and experience packages.

A wide variety of UML modelling tools and risk analysis tools exist and are in use by security analysts and system engineers today. The CORAS platform provides flexible support for integration with such external tools. To this end, the platform provides an integration layer with a defined API which tools can use to integrate with the platform, utilising standardised XML formats for data integration.

The CORAS platform comes with full documentation and provides:

- methodological guidelines in electronic form;
- an advanced tool for table-editing;
- automatic procedures for consistency checking;
- support for generating partly filled in tables based on existing data
- user-guidelines in the form of help functionality.

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	D4.4 The CORAS toolset, guidelines and full documentation (source code)	CO
CORAS Deliverable	D4.5 The CORAS integration platform, the CORAS XML-markup for security assessment, the CORAS vulnerability assessment component	CO
CORAS Deliverable	D5.15 Trial results and assessment of the CORAS methodology	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	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)		6
Number of (public or private) entities potentially involved in the implementation of the result:	11	4
of which : number of SMEs :	1	0
of which : number of entities in third countries (outside EU) :	5	2
Targeted user audience: # of reachable people		> 100 000
# of S&T publications (referenced publications only)	10	20
# of publications addressing general public (e.g. CD-ROMs, WEB sites)	1	10
# of publications addressing decision takers / public authorities / etc.	1	10
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 agreement/Franchising	√	**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.

The CORAS platform and the rest of the CORAS framework is freely available. In particular, the source-code is available as open source on a GNU Lesser General Public License.

All the CORAS results can be downloaded from http://sourceforge.net/projects/coras

SINTEF has a strong commitment to continue development and support of the CORAS integration platform through making use of it as well as enhancing it in other ongoing and future projects. SINTEFs continued investment in the open source platform will thus also benefit other users of the platform as problems are fixed and new features are added.

The open source nature of the platform enables other developers and users to participate in the development of the platform in a number of ways, by contributing bug reports, submitting new code and bug fixes and discussing the platform implementation and usage. Support will be provided through mailing lists and discussion forums, where SINTEF will be an active participant along with other developers and users.

The source code will be hosted at Sourceforge.net. Sourceforge provides a number of services and tools supporting the development and support processes, such as source control systems for coordinating and managing the development process, bug tracking systems, documentation repositories, and forums and mailing lists for discussions.

The platform source code will be maintained in different release series or *branches* as necessary; unstable branches for continued development and adding features, and stable branches focusing on bug fixes to released versions of the platform. This separation enables users to run the platform in a production environment and still be up to date with bug fixes to their stable release without worrying about possible incompatibilities introduced in the most recent development versions.

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 II of this Technological Implementation Plan and I authorise its dissemination to assist this search for collaboration.

Signature: **Name:** Ketil Stølen

Date : August 30, 2003 **Organisation:** SINTEF

Description of Result 6

No. & TITLE OF RESULT

No.	Self-descriptive title of the result
6	***The CORAS XML mark-up for security assessment***

Contact person for this result:

Name	Theodosis Dimitrakos
Position	Senior Scientist
Organisation	CCLRCL
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.CCLRC.ac.uk/
Specific Result URL	http://sourceforge.net/projects/coras

SUMMARY

In the absence of any standardised meta-data format for representing information related to risk assessment, the CORAS consortium has developed an XML mark-up 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 integration platform.

The XML mark-up is also used to facilitate easy integration of risk analysis tools with the CORAS integration platform. In particular, the mark-up defines information models for the core elements of the different risk analysis methods used in CORAS.

Please categorise the result using codes from Annex 1

Subject descriptors codes	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**
CORAS deliverable	D4.5 The CORAS integration platform, the CORAS XML-markup for security assessment, the CORAS vulnerability assessment component	CO
CORAS Deliverable	D5.15 Trial results and assessment of the CORAS methodology.	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			

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:	3	2
of which : number of SMEs :	0	0
of which : number of entities in third countries (outside EU):	2	0
Targeted user audience: # of reachable people		> 100 000
# of S&T publications (referenced publications only)	2	10
# of publications addressing general public (e.g. CD-ROMs, WEB sites)	0	5
# of publications addressing decision takers / public authorities / etc.	0	2
Visibility for the general public	Partly	Partly

[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.

As CCLRC-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 agreement/Franchising	□	**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 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.

CORAS has developed XML-based information models for the core elements of the different risk analysis methods. 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.

The CORAS framework of which this result is a major component is freely available. In particular, the source-code for its computerised components is available as open source on a GNU Lesser General Public License. For additional details on this, see the corresponding section in the Description of Result 5.

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 II of this Technological Implementation Plan and I authorise its dissemination to assist this search for collaboration.

Signature:

Name: Theodosis Dimitrakos

Date: August 30, 2003

Organisation: CCLRCL

Description of Result 7

No. & TITLE OF RESULT

No.	Self-descriptive title of the result
7	*The CORAS vulnerability assessment 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 130
Fax	+ 49 711 866 12 40
E-mail	M.Loupis@SOLINET.com
URL	www.solinet.com
Specific Result URL	http://sourceforge.net/projects/coras

SUMMARY

As networks of hosts continue to grow in size and complexity, evaluating their vulnerabilities that could be exploited becomes increasingly more important preventative measure. Periodic network assessment, used to uncover and correct vulnerabilities, is a common intrusion prevention technique.

Although the tools that perform those assessments, report the same basic information, there are some tool specific differences. Unfortunately, trying to combine output from these tools would require separate parsing tools to address the significant low-level differences.

A standard format for representing assessment information in XML would bring with it the same types of benefits to the vulnerability assessment area with the ones that IDMEF and IODEF are going to bring to the intrusion detection and incident handling areas.

The CORAS vulnerability assessment component addresses this problem. In particular, it proposes a Vulnerability Assessment Report Format (VARF) data model in order to define data formats for sharing information of interest to vulnerability assessment and to facilitate the interaction with the risk management process.

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	D4.5: The CORAS integration platform, the CORAS XML-markup for security assessment, the CORAS vulnerability assessment component	CO
CORAS Deliverable	D5.15 Trial results and assessment of the CORAS methodology	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	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:	6	1
of which : number of SMEs :	1	1
of which : number of entities in third countries (outside EU) :	2	0
Targeted user audience: # of reachable people		>100 000
# of S&T publications (referenced publications only)	0	2
# of publications addressing general public (e.g. CD-ROMs, WEB sites)	0	1
# of publications addressing decision takers / public authorities / etc.	0	5
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

(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 agreement/Franchising	√	**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 framework of which this result is a major component is freely available. In particular, the source-code for its computerised components is available as open source on a GNU Lesser General Public License. For additional details on further dissemination and use, see the corresponding section in the Description of Result 5.

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 II of this Technological Implementation Plan and I authorise its dissemination to assist this search for collaboration.

Signature:	**Name:** Michael Loupis
Date: August 30, 2003	**Organisation:** SOLINET GmbH Telecommunications

Part III - Description of intentions (per partner)

The rest of the document contains Part III of TIP for partners of the CORAS consortium:

- Telenor Communication II AS
- INTRACOM S.A.
- Institute for Energy Technology (IFE)
- Norsk Regnesentral (NR)
- SINTEF
- Norwegian Centre for Telemedicine – University Hospital North Norway
- CCLRC - RAL
- Queen Mary and Westfield College (QMW)
- Research Academic Computer Technology Institute (CTI)
- SOLINET GmbH
- Foundation for Research and Technology – Hellas (FORTH)

CONTRACT NUMBER:	**IST-2000-25031**
PARTNER's NAME:	**Telenor Communication II AS**

CONTACT PERSON:

Name	Erik Dagfinn Wisløff
Position/Title	Senior engineer
Organisation	Telenor Research and Development
Address	Snarøyveien 30, N-1331 Fornebu, Norway
Telephone	+47 909 50 223
Fax	
E-mail	erik-dagfinn.wisloff@telenor.com

Number, TITLE AND BRIEF DESCRIPTION OF MAIN RESULTS

1	*The CORAS framework*
2	*The CORAS methodology for model-based risk assessment (MBRA)*
3	*The CORAS UML profile for security assessment*
4	*The CORAS library of reusable experience packages*
5	*The CORAS integration platform*
6	*The CORAS XML mark-up for security assessment*
7	*The CORAS vulnerability assessment 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	The CORAS MBRA (result 2) will be made available on the Telenor intranet, for optional use by employees conducting a risk analysis of security critical systems. The computerised parts of the CORAS framework will be evaluated for integration with Telenor's existing risk management policies. Successfully passing this business policy focused evaluation, all parts of the framework could be made available for employees conducting risk analysis of security critical systems.	3-6
CORAS User Group	Telenor will be involved in the CORAS User Group, to “give to gain” from the cooperation with other entities using the CORAS framework in full or in part.	0-36

FORESEEN COLLABORATIONS WITH OTHER ENTITIES

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

R&D	Further research or	□	**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 courses	√
JV	Joint venture	□	**CONS**	Available for consultancy	□
			Other	(please specify) *Internal usage*	√

3.2: Quantified data for each partner's main result

Items	Currently achieved quantity [a]	Estimated future quantity [b]
Economic impacts (in EURO)	0	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	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 III of this Technological Implementation Plan and I certify that these are our exploitation intentions

Signature: **Name:** Tony Price

Date: August 30, 2003

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

CONTACT PERSON:

Name	Dimitris 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	*The CORAS methodology for model-based risk assessment (MBRA)*
3	*The CORAS UML profile for security assessment*
4	*The CORAS library of reusable experience packages*
5	*The CORAS integration platform*
6	*The CORAS XML mark-up for security assessment*
7	*The CORAS vulnerability assessment 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	Most departments in the company develop the required software following common Object-Oriented methodologies and process. The security requirements of the developed systems are often very stringent dictating the use of suitable processes that ensure that the final products meet them. It is anticipated that the CORAS framework will be suitable for internal deployment in the Software Development processes followed in the company. It is therefore expected that the integrated CORAS Framework will be incorporated relative easy in the current practises. The gradual deployment of the CORAS framework started from the New Technologies department of INTRACOM. In particular, the CORAS framework will be gradually applied to the security critical components of the CDN project. The first target of assessment will be the Conditional Access module currently at detailed design stage. This module is one of the most security critical components of the project providing the management and control over the users that access the services distributed over the CDN platform. (controls who accesses what and when). The deployment of CORAS framework for the CDN project started beginning of September 2003 in the New Technologies department where a major participant for INTRACOM in the CORAS project (D. Raptis) has recently moved into. The overall effort for assessing security risks in the CDN project is anticipated in the order of 1 Person*Year for approximately one year (Sep. 2004). Following successful completion of the pilot deployment and application of CORAS in the CDN project, an Experience Report will be produced, in the spirit of the reports produced as a result of the trials on the e-Commerce platform. This report will address the Cost/Benefits on the Department, the issues identified for the project, and the decisions taken as a result of the assessments performed.	6-36

	The Experience Report derived as a result of the application of CORAS in the CND project will be circulated in other company departments with software intensive activities. At this stage the most appropriate for further deployment of CORAS seem: • Network Management Systems Department • Defence Department • Wireless Communications Department. To aid the dissemination and adoption of CORAS framework in the individual departments, the CORAS guidelines may be extended or specialised, incorporating examples extracted from the e-Commerce Trials or the CDN project. This will help to clarify and illustrate the specific aspects addressed by each part of the Framework, and it will assist the Software Engineers, as users of the framework, to relate it with their experiences and their application domain. This familiarity may further assist the developers to incorporate the risk analysis techniques within their current practices. Finally, the internal dissemination of the CORAS framework will assist in raising awareness among engineers on the need to address the security aspects of developed systems on early stages of their development.	
Reuse of the assessed mechanisms of the platform	The functionalities assessed in the e-Commerce trials constitute relatively independent security-critical components. These functionalities can therefore become independent reusable components of an assessed security level for integration in future developing systems should the suitable opportunity arise.	6-36
Exploitation of the assessment of e-Commerce platform functionalities	The security mechanisms provided by the e-Commerce platform constitutes an important feature of the platform. The dissemination of the platform's capabilities can be strengthened by emphasising the application of the CORAS framework for the assessment of these security-critical mechanisms.	6-24

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 courses	√
JV	Joint venture	□	**CONS**	Available for consultancy	√
			Other	For internal use	√

3.2: Quantified data for each partner's main result

Items	**Currently achieved quantity** [a]	**Estimated future quantity** [b]
Economic impacts (in EURO)	0	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	1
# of direct jobs safeguarded [c]	1	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 III of this Technological Implementation Plan and I certify that these are currently our main exploitation intentions

Signature: **Name:** D. Raptis

Date: August 30, 2003

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

1	*The CORAS framework*
2	*The CORAS methodology for model-based risk assessment (MBRA)*
3	*The CORAS UML profile for security assessment*
4	*The CORAS library of reusable experience packages*
5	*The CORAS integration platform*
6	*The CORAS XML mark-up for security assessment*
7	*The CORAS vulnerability assessment 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)**
Dissemination and use of the CORAS results 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 (results 1-7)	**(0-30)**
Tutorial on the CORAS methodology for MBRA	In order to promote the use of the CORAS methodology for MBRA, and ease its usability 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, Norway. M1: Tutorial on CORAS MBRA, Presentation, September 2003 M2: Course-material on CORAS MBRA, Report, August 2004 (result 2)	**(0-36)**
CORAS user group in Norway	IFE and SINTEF supported by NST-UNN and Telenor are committed to establish a CORAS user group in Norway. Meetings are planned to take place in Oslo in January 2004 and 2005, and in Halden in September 2004 and 2005. A steering committee with representatives from the four partners will be established. IFE will organise the meetings in Halden. (results 1-7)	**(0-36)**
Consultancy work	IFE will make use of the CORAS results in future consultancy work. Sectors, where IFE is doing consultancy work are within nuclear, petroleum, and transport. Other sectors may also be exploited. (results 1-7)	**(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 courses	√
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	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]	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 III of this Technological Implementation Plan and I certify that these are our exploitation intentions

Signature: **Name: Bjørn Axel Gran**

Date: August 30, 2003

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	*The CORAS framework*
2	*The CORAS methodology for model-based risk assessment (MBRA)*
3	*The CORAS UML profile for security assessment*
4	*The CORAS library of reusable experience packages*
5	*The CORAS integration platform*
6	*The CORAS XML mark-up for security assessment*
7	*The CORAS vulnerability assessment 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. NR's 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. (Results 1-7)	Ongoing
Further R&D project in the area of Computer Security	The CORAS results and the competence gained through the project will be used to propose new project both internally and externally. Application of the CORAS risk analysis methodology and its tool support to real-world problems is an interesting research topic as it could lead to further development of the methodology and the tool. (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 courses	□
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	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	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 III of this Technological Implementation Plan and I certify that these are our exploitation intentions

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

Date: August 30, 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	*The CORAS framework*
2	*The CORAS methodology for model-based risk assessment (MBRA)*
3	*The CORAS UML profile for security assessment*
4	*The CORAS library of reusable experience packages*
5	*The CORAS integration platform*
6	*The CORAS XML mark-up for security assessment*
7	*The CORAS vulnerability assessment 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)**
Dissemination through public seminars in cooperation with the Association of Norwegian ICT- and knowledgebased enterprises	In cooperation with Abelia (Association of Norwegian ICT- and knowledgebased enterprises) representing 330 member companies within: • IT • Telecom • Research • Education • Consultancy SINTEF will present CORAS results at the following public seminars and meetings: September 11: Half day seminar on IT-security including a presentation and demonstration of the CORAS framework. November 4: Parallel session on IT-security at the "Verdi & Viten" conference at the University of Oslo. There will be presentation and demonstration of the CORAS framework. November 26-27: Full day parallel session on IT-security at the AIPro conference at Klætten. There will be presentation and demonstration of the CORAS framework. Janury/February 2004: Another half-day seminar on IT-security. (Results 1-7)	**(0-6)**
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)	**(0-36)**
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)	**(0-36)**

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 The project focuses on CORAS results. In fact, this project will play a major role in the future support of the CORAS open source-code. (Results 1-7)	**(0-36)**
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)	**(0-28)**
MSc and PhD theses	CORAS R&D results will be further developed by several MSc and PhD students. Currently, three PhD students and one MSc student at the University of Oslo do research around CORAS results under supervision by SINTEF personnel. (Results 1-7)	**(0-36)**
Follow-up the ongoing standardisation process for the CORAS UML profile within OMG	Under the leadership of SINTEF, 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”. The proposal has received positive response and was resubmitted both in May and August this year, and will probably be voted on at the OMG meeting in November. (Result 3)	**(0-36)**

Support for the CORAS open source	SINTEF has a strong commitment to continue development and support of the CORAS integration platform through making use of it as well as enhancing it in other ongoing and future projects. SINTEFs continued investment in the open source platform will thus also benefit other users of the platform as problems are fixed and new features are added. The open source nature of the platform enables other developers and users to participate in the development of the platform in a number of ways, by contributing bug reports, submitting new code and bug fixes and discussing the platform implementation and usage. Support will be provided through mailing lists and discussion forums, where SINTEF will be an active participant along with other developers and users. The source code will be hosted at Sourceforge.net. Sourceforge provides a number of services and tools supporting the development and support processes, such as source control systems for coordinating and managing the development process, bug tracking systems, documentation repositories, and forums and mailing lists for discussions. The platform source code will be maintained in different release series or *branches* as necessary; unstable branches for continued development and adding features, and stable branches focusing on bug fixes to released versions of the platform. This separation enables users to run the platform in a production environment and still be up to date with bug fixes to their stable release without worrying about possible incompatibilities introduced in the most recent development versions.	**(0-36)**
CORAS user group in Norway	IFE and SINTEF supported by NST-UNN and Telenor are committed to establish a CORAS user group in Norway. Meetings are planned to take place in Oslo in January 2004 and 2005, and in Halden in September 2004 and 2005. A steering committee with representatives from the four partners will be established. SINTEF will organise the meetings in Oslo. (Results 1-7)	**(0-36)**
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 (fall semester 2003, 2004 &2005), and (2) Modelling with Objects (spring semester 2004, 2005, 2006). (Results 1-7)	**(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 courses	√
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)	500 000	1 000 000
# 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]	2	2
# of direct jobs safeguarded [c]	2	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 III of this Technological Implementation Plan and I certify that these are our exploitation intentions

Signature: **Name: Ketil Stølen**

Date: August 30, 2003

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 RESULTS

1	*The CORAS framework*
2	*The CORAS methodology for model-based risk assessment (MBRA)*
3	*The CORAS UML profile for security assessment*
4	*The CORAS library of reusable experience packages*
5	*The CORAS integration platform*
6	*The CORAS XML mark-up for security assessment*
7	*The CORAS vulnerability assessment 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	NST-UNN is arranging an international workshop on IT-security and risk assessment for the health care sector. Developers of IT systems for the health care sector, as well as risk managers at local GP offices (often GPs), in Norway and other countries are invited to the workshop. The CORAS model-based risk assessment framework will be presented in a tutorial at the workshop. (Results 1-7)	(2-3)
Internal use	NST-UNN is a research and development centre that aims to gather, produce and provide knowledge about telemedicine and ehealth both nationally and internationally. We participate in projects that experiment with innovative ways of utilizing electronic communications in order to improve information flow, work flow and use of resources in the health care sector. In many of the projects we participate with risk assessment, and the CORAS MBRA will be a major candidate for performing risk assessment in the projects. One example of such a project is the **wsHC** (Wireless Health and Care) project. wsHC is an R&D project funded by the Research Council of Norway as an Innovation Project with User-Involvement. One of the work packages is called Security in wireless networks. Our aim is to apply the CORAS results in an appropriate way to reveal security risks. The project started 01.06.03 and lasts through 31.12.05 Another example is the project **Sharing of medication lists** between primary health care and secondary health care institutions. The project is initiated by the Helse Nord RHF, and is planned to start primo 2004. Security will be an essential part of this project, and the CORAS MBRA is a candidate method for performing risk assessment in the project. (Results 1-7)	Ongoing

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
CORAS user group in Norway	IFE and SINTEF supported by NST-UNN and Telenor are committed to establish a CORAS user group in Norway. Meetings are planned to take place in Oslo in January 2004 and 2005, and in Halden in September 2004 and 2005. A steering committee with representatives from the four partners will be established. (Results 1-7)	(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 courses	√
JV	Joint venture	□	**CONS**	Available for consultancy	√
			Other	(Please specify) Internal use	√

3.2: Quantified data for each partner's main result

Items	Currently achieved quantity [a]	Estimated future quantity [b]
Economic impacts (in EURO)	0	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	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 III of this Technological Implementation Plan and I certify that these are our exploitation intentions

Signature: **Name: Eva Skipenes**

Date: August 30, 2003

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	*The CORAS methodology for model-based risk assessment (MBRA)*
3	*The CORAS UML profile for security assessment*
4	*The CORAS library of reusable experience packages*
5	*The CORAS integration platform*
6	*The CORAS XML mark-up for security assessment*
7	*The CORAS vulnerability assessment 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. CCLRC 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 CCLRC is to provide CCLRC 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* CCLRC leading to improvements in the operation and management of CCLRC 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 courses	√
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	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	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 III of this Technological Implementation Plan and I certify that these are our exploitation intentions

Signature: **Name: Theo Dimitrakos**

Date: August 30, 2003

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	*The CORAS methodology for model-based risk assessment (MBRA)*
3	*The CORAS UML profile for security assessment*
4	*The CORAS library of reusable experience packages*
5	*The CORAS integration platform*
6	*The CORAS XML mark-up for security assessment*
7	*The CORAS vulnerability assessment 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)**
MSc and PhD theses	The CORAS R&D work has led to a number of MSc and PhD research projects, as well as several publications at European/International workshops and conferences. It is envisaged that the final results of CORAS will continue to be used as basis for future research work in the department. (Result 1 -6)	Ongoing
University Courses and Training	In view of the importance of security topics the educational market in this area is potentially very large. QMUL 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 would 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 - 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 courses	√
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	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	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 III of this Technological Implementation Plan and I certify that these are our exploitation intentions

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

Date: August 30, 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	*The CORAS methodology for model-based risk assessment (MBRA)*
3	*The CORAS UML profile for security assessment*
4	*The CORAS library of reusable experience packages*
5	*The CORAS integration platform*
6	*The CORAS XML mark-up for security assessment*
7	*The CORAS vulnerability assessment component*

<u>FOR EACH MAIN RESULT:</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)**
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 is interested in extending its consulting services by incorporating the CORAS framework into its programme. However, it does not have the expertise or the tools to do this alone and will explore any relevant collaboration possibilities with potential partners. (Results 1-7)	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 courses	□
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)	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	0
# of direct jobs safeguarded [c]	3 (Result 1)	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 III of this Technological Implementation Plan and I certify that these are our exploitation intentions

Signature: **Name: Sotiris Nikoletseas**

Date: August 30, 2003

CONTRACT NUMBER:	**IST-25031 CORAS**
PARTNER's NAME:	**SOLINET GmbH**

CONTACT PERSON(S):

Name	Michael Loupis
Position/Title	Project Manager
Organisation	SOLINET GmbH
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

Number, TITLE AND BRIEF DESCRIPTION OF MAIN RESULTS

1	*The CORAS framework*
2	*The CORAS methodology for model-based risk assessment (MBRA)*
3	*The CORAS UML profile for security assessment*
4	*The CORAS library of reusable experience packages*
5	*The CORAS integration platform*
6	*The CORAS XML mark-up for security assessment*
7	*The CORAS vulnerability assessment component [*Vulnerability assessment and threat management tools are common security defence means against multiple threats present in the current networks and systems. These tools provide valuable information that could also be used in many parts of MBRA methodology.]

<u>FOR EACH MAIN RESULT:</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)**
Internal Dissemination	Dissemination of the CORAS Vulnerability and Threat Management methodology to other SOLINET departments	0-12
Experimentation activity	Experimentation with the CORAS Vulnerability and Threat Management methodology on representative test beds	0-24
Introduction in new projects	Utilisation of the CORAS Vulnerability and Threat Management methodology in Network Abuse and Security Surveillance Projects	0-36
Integration in Company Products	Integration of the CORAS Vulnerability and Threat Management tools in the SOLINET SAFIRE test platform	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 courses	√
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)		1 MEuro
# of licenses issued (within EU)		10
# of licenses issued (outside EU)		2
Total value of licenses (in EURO)		1 MEuro
# of entrepreneurial actions (start-up company, joint ventures…)		
# of direct jobs created [c]		4
# of direct jobs safeguarded [c]	2	4
# of direct jobs lost		

[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 III of this Technological Implementation Plan and I certify that these are our exploitation intentions

Signature: **Name: Michael Loupis**

Date: 30 August 2003

CONTRACT NUMBER:	**IST-2000-25031**
PARTNER’s NAME:	**Foundation for Research and Technology – Hellas (FORTH)**

CONTACT PERSON:

Name	Manolis Tsiknakis
Position/Title	Researcher, Coordinator of the Center of Medical Informatics and Health Telematics Applications.
Organisation	Institute of Computer science, FORTH
Address	Vassilika Vouton, P.O.Box 1385, Heraklion, Crete, Greece
Telephone	+30 2810391690
Fax	+30 2810391601
E-mail	tsiknaki@ics.forth.gr

Number, TITLE AND BRIEF DESCRIPTION OF MAIN RESULTS

1	*The CORAS framework*
2	*The CORAS methodology for model-based risk assessment (MBRA)*
3	*The CORAS UML profile for security assessment*
4	*The CORAS library of reusable experience packages*
5	*The CORAS integration platform*
6	*The CORAS XML mark-up for security assessment*
7	*The CORAS vulnerability assessment 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 results 2, 4 and 5 will be suitable for internal deployment in the Software Development processes and other R&D activities in ICS-FORTH. As software in ICS-FORTH is developed following Object-Oriented methodologies, it is expected that the "CORAS methodology for MBRA" (result 2) and "UML profile for security assessment" (result 3) will be relative easy incorporated in the current practice. (Results 2, 3, 4, 5)	12 - 18
Reuse of the assessed mechanisms of the tele-medicine services	CORAS framework has been tested through 3 tele-medicine trials. The functionalities assessed in the tele-medicine trials constitute relatively independent security-critical components of telemedicine services. These trials have produced many public and internal Reusable Elements (result 4) that may be suitable in assessing the risks of critical components with similar functionalities. (Result 4)	12
Exploitation of assessment of tele-cardiology and home care services	The security improvements of the tele-cardiology and home care services constitute an important marketing feature. The dissemination of these tele-medicine services can be strengthened by advertising the assessment of various incorporated security-critical mechanisms via the application of the CORAS framework.	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 courses	√
JV	Joint venture	□	**CONS**	Available for consultancy	□
			Other	(please specify) *Internal usage*	√

3.2: Quantified data for each partner's main result

Items	Currently achieved quantity [a]	Estimated future quantity [b]
Economic impacts (in EURO)	0	0
# of licenses issued (within EU)	250,000[1]	1,500,000[1]
# 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	2
# of direct jobs safeguarded [c]	0	0
# of direct jobs lost	0	0

[1] The achieved quantity and estimated future quantity refers to licences achieved and expected regarding the eHealth technological platform of ICS-FORTH, which integrates and utilises security features and methodologies identified using the CORAS risk analysis and assessment framework. Thus, it is an indirect but related exploitation of the CORAS framework on behalf of FORTH.

[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 III of this Technological Implementation Plan and I certify that these are our exploitation intentions

Signature: **Name: Manolis Tsiknakis**

Date: August 30, 2003