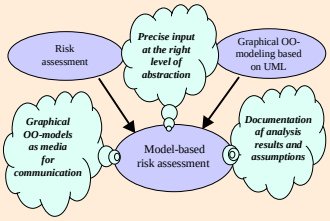
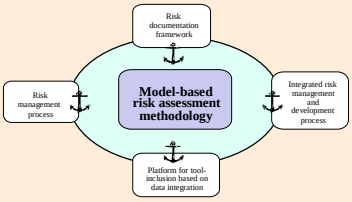
The CORAS Rationale

Model-based risk assessment employs modelling technology for three main purposes:

- To describe the target of assessment at the right level of abstraction
- As a medium for communication and interaction between different groups of stakeholders involved in risk assessment
- To document risk assessment results and the assumptions on which these results depend



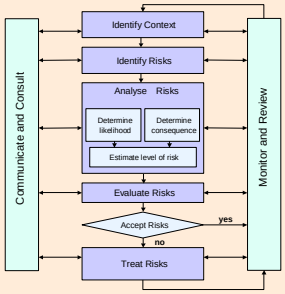


The CORAS Framework

The risk management process provides the core for the CORAS process from a traditional risk analysis background. Combined with the risk documentation framework this provides the basis for the development of the integrated risk management and development process. The fourth anchor point represents the CORAS platform, which is a tool that is interoperable with different other tools from both the risk analysis field and the modelling world, providing a model-based risk assessment product that can be used on either existing systems or systems under development.

The risk management process

The risk management process in CORAS is based on the AS/NZS:4360 standard. This standard divides the process into the five sub-processes mentioned in the figure.



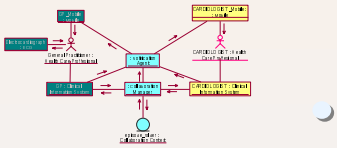
Telemedicine in the CORAS project

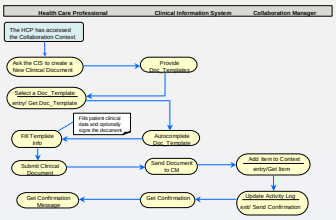
Sub-process 1: Context Identification

Assets	Security requirements
•Patient's health •Medical data •Username&password •Reputation of GP •Medical Equipment •Reputation of system provider •Server software	•**Integrity** of medical info •**Accountability** (identification and non-repudiation) of medical data •**Availability** of service whenever it is needed •**Confidentiality** of the medical information •**Prevention from damage** of equipment and software

Preparatory work, performed by medical experts and technical developers

Context models and descriptions



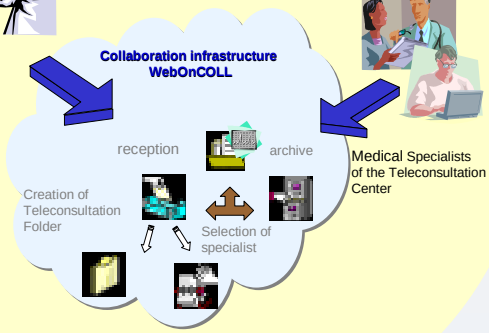


Results from preparatory work presented in a walk-through and used as background for a brainstorming session, identifying threats and unwanted incidents.

Medical experts and technical developers play the most important roles.

Integrated teleconsultation services in cardiology

General Practitioner in Remote healthcare Center



For each risk (group of risks) treatment approaches and options are described.

Sub-process 5: Risk Treatment

Possible approaches

a) Risk avoidance
b) Reduction of likelihood
c) Reduction of consequence
d) Risk transfer
e) Risk retention

Possible treatment options

- Changes to security requirements
- Changes to security policies, for example policies for change of passwords
- Changes to system architecture
- Strategies for testing
- Strategies for monitoring

Risk	Approach	Treatment option	Benefit	Cost
Lack of power supply	a)	Install UPS and generators everywhere	Power problems will not have effect on the service anywhere	Cost of UPS and generator
	b)	N/A		
	c)	Install UPS and gen.s where needed	Power problems will not have effect on service at places with UPS/gen.s installed	Cost of UPS and generator
	d)	N/A		
	e)	No treatment	No benefit	Maybe extra cost due to delay

Sub-process 4: Risk Evaluation

Examples of risk categorisation groups:

- Protection of human life and people's safety
- Integrity of Medical data
- Prevention from unauthorized use of the service
- Reputation of the stakeholders
- Network availability
- Medical expert availability
- Room and equipment availability
- Power availability

Risk level matrix					
	Likelihood				
Consequence	*Rare*	*Unlikely*	*Possible*	*Likely*	*Almost certain*
Minor			50		
Moderate		53	68		
Major	27, 28				

Risk level:	Treatment recommendations:
Extreme risk	Significant improvement of system security necessary
High risk	Senior management must consider if service can be continued
Moderate risk	Specify management responsibility for monitoring the risks
Low risk	Risks can be managed by routine procedures

Risk levels are determined by the combination of consequence and likelihood. The risk level for each unwanted incident is plotted into the Risk Level Matrix.

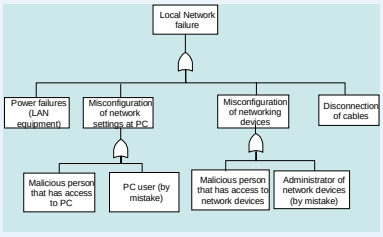
In order to facilitate risk treatment, a categorisation/grouping of risks is performed.

Sub-process 2: Risk Identification

HAZOP

ID	*Assets*	*Guidewords*	*Threats*	*Unwanted incidents*	*Consequence description*
27	Medical data	Manipulation	Medical data is changed in an unauthorised manner	Medical data changed while transmitted to/from server	May cause wrong advice/treatment
28				Medical data changed while stored on server	May cause wrong advice/treatment
50		Unavailability	Information on server is unavailable	Information is unavailable for Cardiologist for more than 5 minutes	A delay for the Cardiologist
53				Information on server is permanently unavailable	Information is lost if insufficient backup routines
68			Lack of power supply at end points.	Power supply goes down at PHCC	TeleCardiology service cannot be used

FTA (Fault Tree Analysis)



Sub-process 3: Risk Analysis

Examples of consequence values

Consequence value	Description
Minor	• Unavailability of hardware/software that is possible to be bypassed.
Moderate	• Unavailability of the teleconsultation service. • Disclosure of patient data.
Major	• Violation of the integrity of the medical data that may cause problems to patient's life or stakeholder's reputation (legal and moral consequences) •Unauthorised use of the system in order to request/provide medical advice (accountability).

Examples of likelihood definitions

Likelihood descriptor	Probability range
Rare	0.00 – 0.01
Unlikely	0.02 – 0.05
Possible	0.06 – 0.20
Likely	0.21 – 0.50
Almost certain	0.51 – 1.00

Values for consequence and likelihood are assigned for each unwanted incident. This is done by medical experts and technical developers and in accordance with definitions they have made.

CORAS

Risk Assessment of Security Critical Systems

Please contact us

Ketil Stølen
SINTEF Telecom and Informatics
ketil.stoelen@sintef.no

Tony Price
Telenor Research and Development
price@transtrad.com

http://www.nr.no/coras

The Consortium

The CORAS consortium consists of three commercial companies:
- Intracom (Greece),
- Solinet (Germany) and
- Telenor (Norway);

seven research institutes:
- CLRC/RAL (UK),
- CTI (Greece),
- FORTH (Greece),
- IFE (Norway),
- NST (Norway),
- NR (Norway) and
- SINTEF (Norway);

as well as one university college:
- Queen Mary University of London (UK).