The CORAS approach to model-driven risk analysis

RISE presentation
May 13, 2011

Atle Refsdal, SINTEF
Outline

- General introduction
  - what is risk analysis, definition of terms, …

- Overview of the CORAS process and risk modeling language

- The eight steps of a CORAS risk analysis

- Small demo/exercise?
What is risk analysis?

- Determining what can happen, why and how
- Systematic use of available information to determine the level of risk
- Prioritisation by comparing the level of risk against predetermined criteria
- Selection and implementation of appropriate options for dealing with risk
Terms

- Asset, something of value
- Vulnerability
- Threat

Risk with respect to security

Need to introduce security mechanisms

Reduced security risk
Definition of Terms

- **Asset**: Something to which a party assigns value and hence for which the party requires protection
- **Consequence**: The impact of an unwanted incident on an asset in terms of harm or reduced asset value
- **Likelihood**: The frequency or probability of something to occur
- **Party**: An organization, company, person, group or other body on whose behalf a risk analysis is conducted
- **Risk**: The likelihood of an unwanted incident and its consequence for a specific asset
- **Threat**: A potential cause of an unwanted incident
- **Threat scenario**: A chain or series of events that is initiated by a threat and that may lead to an unwanted incident
- **Treatment**: An appropriate measure to reduce risk level
- **Unwanted incident**: An event that harms or reduces the value of an asset
- **Vulnerability**: A weakness, flaw or deficiency that opens for, or may be exploited by, a threat to cause harm to or reduce the value of an asset
Risk management is the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects.

Our focus: Risk Analysis
Elements of risk analysis

- **Context**: Vulnerability
- **Target**: Threat, Unwanted Incident
- **Asset**: Frequency, Consequence
- **Treatment**: Risk
The CORAS process

- Risk management process based on **ISO 31000**: Risk Management – Principles and Guidelines
- Provides *process* and *guidelines* for risk analysis
Context identification

- Characterise target of analysis
  - What is the focus and scope of the analysis?

- Identify and value assets
  - Asset-driven risk analysis process
  - Business oriented, e.g. availability of services generating revenue

- Specify risk evaluation criteria
  - There will always be risks, but what losses can the client tolerate?
  - Similar to requirements in system development
Risk identification

- Identify threats to assets through structured brainstorming
  - Hazard and Operability analysis (HazOp)
  - Involving system owners, users, developers, domain experts, risk analysis experts, etc. (typically 5-7 people)

- Identify vulnerabilities of assets
  - Questionnaires and checklists

---

**Equipment physical security**

- Is equipment properly physically protected against unauthorised access to data or loss of data?
- Are power supplies handled in a manner that prevents loss of data and ensures availability?
- …
Risk evaluation

- We cannot completely eliminate all risks
- Determine which risks need treatment
  - We need to know how serious they are so we can prioritise

- Risk level is determined based on analysis of the likelihood and consequence of the unwanted incident
  - Quantitative values: e.g., loss of 1M€, 25% chance per year
  - Qualitative values: e.g., high, medium, low
Risk treatment

- Identify treatments for unaccepted risks
- Evaluate and prioritise different treatments
Model-based risk analysis

- Precise input at the right level of abstraction
- Graphical models as media for communication
- Documentation of analysis results and assumptions

Risk analysis

Graphical modelling
What is CORAS?

- The CORAS process
  - A process for security risk analysis
- The CORAS language (diagrams)
  - A graphical language that supports the analysis process
  - Basis for communication, documentation and analysis
- The CORAS semantics
  - A schematic translation of any CORAS diagram into English
- The CORAS guideline
  - A guideline for best use of the language within the process
- The CORAS tool
  - A computerized tool supporting the above
The CORAS language
The CORAS diagrams

- **Asset diagrams**
  Describes the focus of the analysis

- **Threat diagrams**
  Describes scenarios which may cause harm to the assets

- **Risk diagrams**
  Summarises the risks presented in threat diagrams

- **Treatment diagrams**
  Adds proposed treatments to threat diagrams

- **Treatment overview diagrams**
  Adds proposed treatments to risk diagrams
Threat Diagram – Example 1

Threat: Burglar
Vulnerability: Unlocked window
Threat scenario: Burglar enters house through window
Unwanted incident: Burglar steals jewelry
Treatment: Install a window lock
Deposit jewelry in safe-deposit box
Asset: Jewelry
Place a guard dog in the yard
Threat Diagram – Example 2

- Power supply in Sweden breaks down [1:5 years]
- Power supply in Norway breaks down [1:100 years]
- Blackout in Norway [3:100 years]
- Power production in Norway critical

Threat: Hacker
Threat scenario: Power supply in Norway breaks down
Unwanted incident: Blackout in Norway
Asset: Power production in Norway
Semantics: Translation into English

Vertices
- *Hacker* is a deliberate human threat.
- Threat scenario *Power supply in Norway breaks down* occurs with undefined likelihood.
- Threat scenario *Power supply in Sweden breaks down* occurs with likelihood 1:5 years.
- Unwanted incident *Blackout in Norway* occurs with likelihood 3:100 years.
- *Power production in Norway* is a direct asset.

Relations
- *Hacker* initiates *Power supply in Norway breaks down* with likelihood 1:100 years.
- *Power supply in Norway breaks down* leads to *Blackout in Norway* with conditional likelihood 1.0.
- *Power supply in Sweden breaks down* leads to *Blackout in Norway* with conditional likelihood 0.1.
- *Blackout in Norway* impacts *Power production in Norway* with consequence *critical*. 
Identifying and documenting assets

- **Asset:** Something to which a party assigns value and hence for which the party requires protection
- The client specifies its assets and risk acceptance levels
- Difficult, - faults may jeopardize the whole analysis
  - wrong focus
  - wrong level of details

![Diagram with client, product information, budget, and business contracts]
Identifying and documenting assets

- One may also specify other interested parties than the client
  - Different parties may have different assets
  - Two parties may assign value to the same parts or aspects (e.g. confidentiality), but possibly with different priority (asset value) and different protection requirements

- Possible to specify how assets can depend on other assets
  - company reputation
  - income

![Diagram showing dependencies between assets](image)
Identifying and documenting threats and unwanted incidents in threat diagrams

**Threat:** A *potential cause of an unwanted incident*

**Unwanted incident:** *An event that harms or reduces the value of an asset*

<table>
<thead>
<tr>
<th>Threat</th>
<th>Unwanted incident</th>
<th>Asset damaged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus</td>
<td>Virus attack makes information unavailable</td>
<td>Business contracts</td>
</tr>
<tr>
<td>Virus</td>
<td>Virus attack makes information unavailable</td>
<td>Product information</td>
</tr>
<tr>
<td>Employee</td>
<td>Product information is accidentally published on the web</td>
<td>Product information</td>
</tr>
<tr>
<td>Insider</td>
<td>Competitor receives confidential information</td>
<td>Product information</td>
</tr>
<tr>
<td>Insider</td>
<td>Competitor receives confidential information</td>
<td>Budget</td>
</tr>
</tbody>
</table>
Identifying and documenting vulnerabilities and threat scenarios

- **Vulnerability**: A weakness, flaw or deficiency that opens for, or may be exploited by, a threat to cause harm to or reduce the value of an asset.
- **Threat scenario**: A chain or series of events that is initiated by a threat and that may lead to an unwanted incident.
- Forces the participants to specify “why” incidents can happen (vulnerabilities) and “how” (threat scenarios).

**Diagram**:
- Virus
- Insufficient virus protection
- Information system is attacked
- Wrong information is selected for publication
- No warning
- Confident information is downloaded anonymously
- Information is sold
- Confidential information is downloaded anonymously
- Employee
- Access to confidential information
- Insider
- No logging
- Product information is accidentally published on the web
- Virus attack makes information unavailable
- Competitor receives confidential information
- Business contracts
- Product information
- Budget
Identifying and documenting likelihoods and consequences

- **Likelihood:** The frequency or probability of something to occur
- **Consequence:** The impact of an unwanted incident on an asset in terms of harm or reduced asset value
Documenting risks

- **Risk**: The likelihood of an unwanted incident and its consequence for a specific asset
- Compared to the party’s risk acceptance levels
- Acceptable and non-acceptable risks are shown in a risk diagram
  - decision makers
  - planning treatments
  - communicating risks

[Diagram showing various risks and their consequences, including:
- Risk 1: Virus attack makes information unavailable [unacceptable]
- Risk 2: Virus attack makes information unavailable [acceptable]
- Risk 3: Product information is accidentally published on the web [unacceptable]
- Risk 4: Competitor receives confidential information [unacceptable]
- Risk 5: Competitor receives confidential information [acceptable]]
Identifying and documenting risk treatments

- Risks that are *unacceptable* are evaluated to identify appropriate treatments
- Risks that are *acceptable* can be removed from the diagram
Identifying and documenting risk treatments

- Risk treatment: An appropriate measure to reduce risk level
- Treatments are added where they should have effect

- Risk 1: Virus attack makes information unavailable [unacceptable]
- Risk 3: Product information is accidentally published on the web [unacceptable]
- Risk 4: Competitor receives confidential information [unacceptable]
Example CORAS diagrams
Example asset diagram

- Party
- Indirect asset
- Harm relation
- Asset

Company

Company’s reputation

Integrity of server [high]
Confidentiality of information [critical]
Availability of server [critical]
Example threat diagram

Unwanted incident

Hacker gets access to server [unlikely]

Consequence

Confidentiality of information [high]

Integrity of server [high]

Availability of server [high]

Server is infected by computer virus [possible]

Vulnerability

Threat

Virus protection not up to date

Computer virus

Likelihood

Threat scenario

Impacts relation

0.1

0.2
Example risk diagram

HA: Hacker gets access to server [unacceptable]

VB: Virus creates back door to server [unacceptable]

SD2: Server goes down [acceptable]

SD1: Server goes down [unacceptable]

Confidentiality of information

Integrity of server

Availability of server

Risk level

Risk

Initiates relation

Leads-to relation
Example treatment diagram

Treats relation

Implement new routines for updating virus protection

Reduce likelihood

Reduce consequence

Install monitoring software

Treatment scenario

Treatment category

Confidentiality of information

Integrity of server

Availability of server

SD1: Server goes down [unacceptable]

SD2: Server goes down [acceptable]

VB: Virus creates back door to server [unacceptable]

HA: Hacker gets access to server [unacceptable]

Server is infected by computer virus [possible]

Computer virus

Virus protection not up to date
Example treatment overview diagram
Building a threat diagram (1)

Threat

Employee

Asset

Data integrity
Building a threat diagram (2)

Employee

- Initiates relation
  - Unwanted incident
  - Corruption of data
  - Data integrity

- Impacts relation
Building a threat diagram (3)

- Employee
- Old antivirus
- Malicious code spreads via LAN
- Old firewall
- Malicious code traffic jams network
- Old version of webserver
- Vulnerability
- Threat scenario
- Servers infected
- Servers malfunctioning
- Corruption of data
- Data integrity
Building a threat diagram (4)

- Employee
- Malicious code spreads via LAN [1 per year]
- Old antivirus
- Old firewall
- Malicious code traffic jams network [1 per year]
- Old version of webserver
- Servers infected [1 per 10 years]
- Servers malfunctioning [1 per 5 years]
- Data integrity
- Correlation of data [1 per year]

Likelihood

Risk

Consequence
The eight steps of a CORAS risk analysis

1. Customer presentation of target
2. Approval of target description
3. Preparation for the analysis
4. Risk estimation using threat diagrams
5. Refining the target description using asset diagrams
6. Risk estimation using threat diagrams
7. Risk identification using threat diagrams
8. Risk evaluation using risk diagrams

SINTEF
Step 1: Preparation

- The purpose of Step 1 is to do the necessary initial preparations prior to the actual startup of the analysis.

- This includes:
  - Roughly setting the scope and focus.
  - Informing the customer of its responsibilities.
Step 2: Customer presentation

- The second step involves an introductory meeting
- The main item on the agenda for this meeting is to get the representatives of the client to present their overall goals of the analysis and the target they wish to have analysed
- Hence, during the initial step the analysts will gather information based on the customer's presentations and discussions
Tasks

- The security analysis method is introduced
- The customer presents the goals and the target of the analysis
- The focus and scope of the analysis is set
- The meetings and workshops are planned
People that should participate

- Analysis leader (required)
- Analysis secretary (required)
- Representatives of the customer:
  - Decision makers (required)
  - Technical expertise (optional)
  - Users (optional)
Modelling guideline

- At this early stage of the analysis it can be useful to describe the target with informal drawings, pictures or sketches on a blackboard
- The presentation can later be supplemented with more formal modelling techniques such as UML or data flow-diagram
Telemedicine case
Step 3: Refining the target

- The third step also involves a separate meeting with representatives of the customer.
- However, this time the analysts will present their understanding of what they learned at the first meeting and from studying documentation that has been made available to them by the client.
- The third step also involves a rough, high-level security analysis.
- During this analysis the first threats, vulnerabilities, threat scenarios and unwanted incidents are identified.
- They will be used to help directing and scoping the more detailed analysis still to come.
Tasks

- The target as understood by the analysts is presented
- The assets are identified
- A high-level analysis is conducted
People that should participate

- Security analysis leader (required)
- Security analysis secretary (required)
- Representatives of the customer:
  - Decision makers (required)
  - Technical expertise (required)
  - Users (optional)
Modelling guideline for the target description

- Use a formal or standardised notation such as UML, but ensure that the notation is explained thoroughly so that the participants understand it.
- Create models of both the static and the dynamic features of the target.
- Static may be hardware configurations, network design etc., while dynamic may be work processes, information flow etc.
- For the static parts of the description UML class diagrams and UML collaboration diagrams (or similar notations) are recommended.
- For the dynamic parts we recommend UML activity diagrams and UML sequence diagrams (or similar notations)
Symbols from the CORAS risk modelling language
Asset diagram

Ministry of health

Provision of telecardiology service

Patients’ health

Health records

Public’s trust in system
# High-level risk table

<table>
<thead>
<tr>
<th>Who/what causes it?</th>
<th>How? What is the incident? What does it harm?</th>
<th>What makes it possible?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacker</td>
<td>Breaks into the system and steals health records</td>
<td>Insufficient security</td>
</tr>
<tr>
<td>Employee</td>
<td>Sloppiness compromises confidentiality of health records</td>
<td>Insufficient training</td>
</tr>
<tr>
<td>Eavesdropper</td>
<td>Eavesdropping on dedicated connection</td>
<td>Insufficient protection of connection</td>
</tr>
<tr>
<td>System failure</td>
<td>System goes down during examination</td>
<td>Unstable connection/immature technology</td>
</tr>
<tr>
<td>Employee</td>
<td>Sloppiness compromises integrity of health record</td>
<td>Prose-based health records</td>
</tr>
<tr>
<td>Network failure</td>
<td>Transmission problems compromises integrity of medical data</td>
<td>Unstable connection/immature technology</td>
</tr>
<tr>
<td>Employee</td>
<td>Health records leaks out by accident, compromises their confidentiality and damages the trust in the system</td>
<td>Possibility of irregular handling of health records</td>
</tr>
</tbody>
</table>
Step 4: Approval

- The fourth step involves a more refined description of the target to be analysed, and also
  - all assumptions being made and
  - other preconditions made
- Step 4 is terminated once all this documentation has been approved by the customer
Tasks

- The client approves target descriptions and asset descriptions
- The assets should be ranked according to importance.
- Consequence scales must be set for each asset within the scope of the analysis
- A likelihood scale must be defined
- The client must decide risk evaluation criteria for each asset within the scope of the analysis
People that should participate

- The same as in the previous meeting, but since this step sets the boundaries for the further analysis it is important that the relevant decision-makers are present.
## Asset table

<table>
<thead>
<tr>
<th>Asset</th>
<th>Importance</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health records</td>
<td>2</td>
<td>Direct asset</td>
</tr>
<tr>
<td>Provision of telecardiology service</td>
<td>3</td>
<td>Direct asset</td>
</tr>
<tr>
<td>Public’s trust in system</td>
<td>2</td>
<td>Indirect asset</td>
</tr>
<tr>
<td>Patients’ health</td>
<td>1</td>
<td>Direct asset</td>
</tr>
</tbody>
</table>
## Consequence scale for health records

<table>
<thead>
<tr>
<th>Consequence value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>1000+ health records are affected</td>
</tr>
<tr>
<td>Major</td>
<td>101–1000 health records are affected</td>
</tr>
<tr>
<td>Moderate</td>
<td>11–100 health records are affected</td>
</tr>
<tr>
<td>Minor</td>
<td>1–10 health records are affected</td>
</tr>
<tr>
<td>Insignificant</td>
<td>No health records are affected</td>
</tr>
</tbody>
</table>
## Likelihood scale

<table>
<thead>
<tr>
<th>Likelihood value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certain</td>
<td>Five times or more per year</td>
<td>$[50, \infty) : 10y = [5, \infty) : 1y$</td>
</tr>
<tr>
<td>Likely</td>
<td>Two to five times per year</td>
<td>$[20, 50) : 10y = [2, 5) : 1y$</td>
</tr>
<tr>
<td>Possible</td>
<td>Less than twice per year</td>
<td>$[5, 20) : 10y = [0.5, 2) : 1y$</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Less than once per two years</td>
<td>$[1, 5) : 10y = [0.1, 0.5) : 1y$</td>
</tr>
<tr>
<td>Rare</td>
<td>Less than once per ten years</td>
<td>$[0, 1) : 10y = [0, 0.1) : 1y$</td>
</tr>
</tbody>
</table>
Risk evaluation matrix

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step 5: Risk identification

- This step is organised as a workshop gathering people with expertise on the target of evaluation.
- The goal is to identify as many potential unwanted incidents as possible, as well as threats, vulnerabilities and threat scenarios.
Tasks

- The initial threat diagrams should be completed with identified threats, vulnerabilities, threat scenarios and unwanted incidents.
People that should participate

- Security analysis leader (required)
- Security analysis secretary (required)
- Representatives of the client:
  - Decision makers (optional)
  - Technical expertise (required)
  - Users (required)
Initial threat diagram: accidental actions

- Insufficient training
- Prose-based health records
- Possibility of irregular handling of health records
  
- Sloppy handling of records
  - Compromise of confidentiality of health records
  
- Health record leakage
  - Compromise of integrity of health records
  
- Health records

Employee
Initial threat diagram: deliberate actions

Hacker

Insufficient security

Eavesdropper

Insufficient protection of connection

System break-in

Eavesdropping on dedicated connection

Health records theft

Compromise of confidentiality of data transmitted

Health records
Initial threat diagram: non-human threats

- System failure
- Network failure
- Immature technology
- Unstable connection
- System goes down during examination
- Examination disrupted
- Provision of telecardiology service
- Compromise of integrity of medical data
- Health records
Final threat diagram: accidental actions

- Health records sent to unauthorised people
  - Possibility of irregular handling of health records
  - Compromise of confidentiality of health records
- Health record copies stored on local computer
  - Insufficient training
  - Prose-based health records
  - Wrong input in health record
  - No input validation
  - Compromise of integrity of health records
  - Patient is given wrong diagnosis
  - Unable to set diagnosis due to slow system
  - Slow system
  - Provision of telecardiology service
- IT
  - Insufficient personnel
  - Access control
  - Lack of competence
  - Misconfiguration of system
Step 6: Risk estimation

- The sixth step is also organised as a workshop
- This time with focus on estimating consequences and likelihood values for each of the identified unwanted incidents
Tasks

- Threat scenarios must be given a likelihood estimate and likelihoods for unwanted incidents are based on these.
- Every relation between an unwanted incident and an asset must be given a consequence estimate.
People that should participate

- Security analysis leader (required)
- Security analysis secretary (required)
- Representatives of the client:
  - Decision makers (required)
  - Technical expertise regarding the target (required)
  - Users (required)
Modelling guideline

Risk estimation on threat diagrams:
- Add likelihood estimates to the threat scenarios.
- Add likelihood estimates to the unwanted incidents, based on the threat scenarios.
- Annotate each unwanted incident-asset relation with a consequence taken from the respective asset's consequence scale.
Threat diagram with estimates

- Health records sent to unauthorised people [rare]
- Compromise of confidentiality of health records [rare]
- Compromise of integrity of health records [possible]
- Patient is given wrong diagnosis [unlikely]
- Unable to set diagnosis due to slow system [likely]
- Slow system [possible]
- Provision of telecardiology service

Possiblecauses:
- Possibility of irregular handling of health records
- Insufficient training
- Prose-based health records
- No input validation
- Wrong input in health record [possible]
- Misconfiguration of system [possible]
- Insufficient personnel access control competence

- Health records moderate
- Patients’ health major
- Provision of telecardiology service moderate
- Compromise of confidentiality of health records moderate
- Patient is given wrong diagnosis catastrophic
## Combined likelihood estimates

<table>
<thead>
<tr>
<th>Threat scenario</th>
<th>Likelihood</th>
<th>Unwanted incident</th>
<th>Combined likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health records sent to unauthorised people</td>
<td>Rare ($[0, 1): 10y$)</td>
<td>Compromise of confidentiality of health records</td>
<td>$[0, 1): 10y + [1, 5): 10y = [1, 6): 10y$</td>
</tr>
<tr>
<td>Health record copies stored on local computer</td>
<td>Unlikely ($[1, 5): 10y$)</td>
<td></td>
<td>It is decided that unlikely is the best fit</td>
</tr>
</tbody>
</table>
Step 7: Risk evaluation

- This step involves giving the client the first overall risk picture
- This will typically trigger some adjustments and corrections
Tasks

- Likelihood and consequence estimates should be confirmed or adjusted
- The final adjustments of the acceptable area in the risk matrices should be made (if needed)
- An overview of the risks may be given in a risk diagram
People that should participate

- Security analysis leader (required)
- Security analysis secretary (required)
- Representatives of the client:
  - Decision makers (required)
  - Technical expertise regarding the target (optional)
  - Users (optional)
Risk evaluation matrix with risks

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare</td>
<td></td>
<td></td>
<td>CC1, CC1(I)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PRI</td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td>CII(I), SS1(I)</td>
<td>CII, SS1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SS2</td>
</tr>
<tr>
<td>Certain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Risk overview diagram

CC1: Compromise of confidentiality of health records [acceptable]

CI1: Compromise of integrity of health records [unacceptable]

PR1: Patient is given wrong diagnosis [unacceptable]

SS2: Unable to set diagnosis due to slow system [unacceptable]

SS1: Slow system [unacceptable]

Health records

Patients’ health

Provision of telecardiology service
Step 8: Risk treatment

- The last step is devoted to treatment identification, as well as addressing cost/benefit issues of the treatments.
- This step is best organised as a workshop.
Tasks

- Add treatments to threat diagrams
- Estimate the cost/benefit of each treatment and decide which ones to use
- Show treatments in risk overview diagrams
People that should participate

- Security analysis leader (required)
- Security analysis secretary (required)
- Representatives of the client:
  - Decision makers (required)
  - Technical expertise (required)
  - Users (required)
Treatment diagram
Treatment overview diagram

CI1: Compromise of integrity of health records [unacceptable]

PRI1: Patient is given wrong diagnosis [unacceptable]

SS2: Unable to set diagnosis due to slow system [unacceptable]

SS1: Slow system [unacceptable]

Revise access lists

Extend training program (1–2 days)

GP

IT personnel

Health records

Patients’ health

Provision of telecardiology service
The CORAS web page

- publications
- tool download

http://coras.sourceforge.net/